NETGEAR

N300 Wireless Gigabit Router JNR3000

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

June 2012
202-10989-01
v1.0

© 2012 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2012 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2001
  Safety of information technology equipment
- EN 300 328 V1.7.1 (2006-10)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 489-17 V1.2.1 (2002-08) and EN 301 489-1 V1.4.1 (2002-08)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries under the following conditions and/or with the following restrictions:

- In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
- This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	[NETGEAR Inc.] tímto prohlašuje, že tento [JNR3000] je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.

da Dansk [Danish]	Undertegnede [NETGEAR Inc.] erklærer herved, at følgende udstyr [JNR3000] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt [NETGEAR Inc.], dass sich das Gerät [JNR3000] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab [NETGEAR Inc.] seadme [JNR3000] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, [NETGEAR Inc.], declares that this [JNR3000] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente [NETGEAR Inc.] declara que el [JNR3000] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [NETGEAR Inc.] ΔΗΛΩΝΕΙ ΟΤΙ [JNR3000] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente [NETGEAR Inc.] déclare que l'appareil [JNR3000] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente [NETGEAR Inc.] dichiara che questo [JNR3000] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [NETGEAR Inc.] deklarē, ka [JNR3000] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [NETGEAR Inc.] deklaruoja, kad šis [JNR3000] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart [NETGEAR Inc.]. dat het toestel [JNR3000] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, [NETGEAR Inc.], jiddikjara li dan [JNR3000] jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, [NETGEAR Inc.] nyilatkozom, hogy a [JNR3000] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym [NETGEAR Inc.] oświadcza, że [JNR3000] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	[NETGEAR Inc.] declara que este [JNR3000] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	[NETGEAR Inc.] izjavlja, da je ta [JNR3000] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[NETGEAR Inc.] týmto vyhlasuje, _e [JNR3000] spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	[NETGEAR Inc.] vakuuttaa täten että [JNR3000] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

SV Svenska [Swedish]	Härmed intygar [NETGEAR Inc.] att denna [JNR3000] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

Radio Frequency Notice: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We NETGEAR, Inc., 350 East Plumeria, San Jose, CA 95134, declare under our sole responsibility that N300 Wireless Gigabit Router JNR3000 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

N300 Wireless Gigabit Router JNR3000

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Contents

Chapter 1 Hardware Setup

Unpack Your Router 10
Position Your Router 10
Hardware Features 11
Front Panel 11
Back Panel 13
Label 13

Chapter 2 Getting Started with NETGEAR Genie

Router Setup Preparation 15
Use Standard TCP/IP Properties for DHCP 15
Gather ISP Information 15
Wireless Devices and Security Settings 15
Types of Logins and Access 15
NETGEAR Genie Setup 16
Use NETGEAR Genie after Installation 17
Upgrade Router Firmware 17
Router Dashboard (Basic Home Screen) 18
Add Wireless Devices or Computers to Your Network 19
Manual Method 19
Wi-Fi Protected Setup (WPS) Method 19

Chapter 3 Genie Basic Settings

Internet Setup 21
Internet Setup Screen Fields 21
Attached Devices 23
Parental Controls 24
Basic Wireless Settings 24
Wireless Settings Screen Fields 25
Change WPA Security Option and Passphrase 26
Guest Networks 27
Guest Network Wireless Security Options 28
FastLane 29

Chapter 4 Genie Advanced Home

Setup Wizard 32
WPS Wizard 33
Setup Menu 34

WAN Setup 35
Default DMZ Server 36
Change the MTU Size 36
LAN Setup 38
LAN Setup Screen Settings 39
Use the Router as a DHCP Server 39
Address Reservation 40
Quality of Service (QoS) Setup 41

Chapter 5 Security

Keyword Blocking of HTTP Traffic 47
Block Services (Port Filtering) 48
Schedule Blocking 50
Security Event Email Notifications 50

Chapter 6 Administration

Upgrade the Router Firmware 53
View Router Status 54
Router Information 54
Internet Provider (WAN) Setup 54
Wireless Settings 57
Guest Network 58
View Logs of Web Access or Attempted Web Access 58
Manage the Configuration File 59
Back Up Settings 60
Restore Configuration Settings 60
Erase 60
Set Password 61
Password Recovery 61

Chapter 7 Advanced Settings

Advanced Wireless Settings 63
Wireless Repeating Function (WDS) 64
Wireless Repeating Function 65
Set Up the Base Station 66
Set Up a Repeater Unit 67
Port Forwarding and Triggering 68
Remote Computer Access Basics 68
Port Triggering to Open Incoming Ports 69
Port Forwarding to Permit External Host Communications 71
How Port Forwarding Differs from Port Triggering 72
Set Up Port Forwarding to Local Servers 72
Add a Custom Service 73
Editing or Deleting a Port Forwarding Entry 74
Set Up Port Triggering 75
Dynamic DNS 77

Static Routes 79
Remote Management 81
Universal Plug and Play 82
Traffic Meter 83

Chapter 8 Troubleshooting

Quick Tips 86
Sequence to Restart Your Network 86
Check Ethernet Cable Connections 86
Wireless Settings 86
Network Settings 86
Troubleshooting with the LEDs 87
Power/Test LED Is Off or Blinking 87
Power/Test LED Stays Amber 87
LEDs Never Turn Off 88
Internet or Ethernet Port LEDs Are Off 88
Wireless LEDs Are Off 88
The Push 'N' Connect (WPS) Button Blinks Amber 88
Cannot Log In to the Router 89
Cannot Access the Internet 89
Troubleshooting PPPoE 91
Troubleshooting Internet Browsing 91
Changes Not Saved 92
Wireless Connectivity 92
Wireless Signal Strength 92
Restore the Factory Settings and Password 93
Troubleshoot Your Network Using the Ping Utility 93
Test the LAN Path to Your Router 93
Test the Path from Your Computer to a Remote Device 94

Appendix A Supplemental Information

Factory Default Settings 96
Specifications 97

Appendix B Notification of Compliance

Index

Hardware Setup

1

Getting to know your router

The N300 Wireless Gigabit Router JNR3000 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (PCs, gaming consoles, and so on) that you connect to your home network.

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 3, Genie Basic Settings*, explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Router*
- *Position Your Router*
- *Hardware Features*

For more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

Unpack Your Router

Open the box and remove the router, cables, and installation guide.

Figure 1. Check the package contents

Your box contains the following items:

- N300 Wireless Gigabit Router JNR3000
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and router setup instructions

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you need to return the product for repair.

Position Your Router

The router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your router:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.

- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, PCs, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

Hardware Features

Before you cable your router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The router front panel has the status LEDs and icons shown in the following figure.

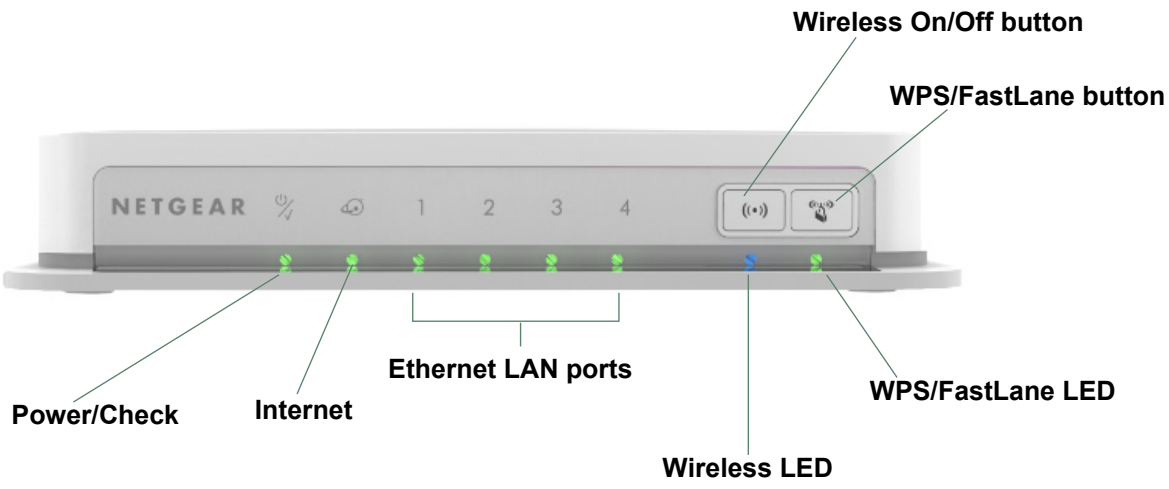


Figure 2. Router, front view

Table 1. Front panel LED descriptions

LED	Description
Power/Test	• **Solid green**. The startup is completed, and the router is ready. • **Blinking green**. The firmware is corrupted (see http://www.netgear.com/support). • **Blinking amber**. The firmware is upgrading, or the **Reset** button was pressed. • **Off**. Power is not supplied to the router.
Internet	• **Solid green**. An IP address has been received; ready to transmit data. • **Solid amber**. An Ethernet cable connection to the modem has been detected. • **Off**. No Ethernet cable is connected to the modem.
LAN ports 1–4	• **Solid green**. The local port is connected to a 1000 Mbps device. • **Blinking green**. Data is being transmitted at 1000 Mbps. • **Solid amber**. The local port is connected to a 10/100 Mbps device. • **Blinking amber**. Data is being transmitted at 10/100 Mbps. • **Off**. No link is detected on this port.
Wireless	• **Solid blue**. The wireless interface is enabled. • **Blinking blue**. Data is being communicated over the wireless network. • **Off**. The wireless interface is turned off.
WPS	• **Solid green**. A WPS-capable device has been accepted by the router and is ready to be used. • **Blinking green**. The WPS-capable device will be associated with the router within 2 minutes. • **Off**. No WPS connection exists.

The WLAN and WPS buttons toggle the WLAN and WPS functions on and off.

- **Wireless On/Off button**. Pressing and holding the wireless LAN button for 2 seconds turns the 2.4 GHz wireless radio on and off. If the Wireless LED is lit, the wireless radio is on. If the LED is off, then the wireless radio is turned off and you cannot connect wirelessly to the router.
- **WPS button**. You can use this button to use WPS to add a wireless device or computer to your wireless network. The LED below the WPS button blinks green when the router is trying to add the wireless device or computer. The LED stays solid green when wireless security is enabled in the router.

Back Panel

The back panel has the connections shown in the following figure.

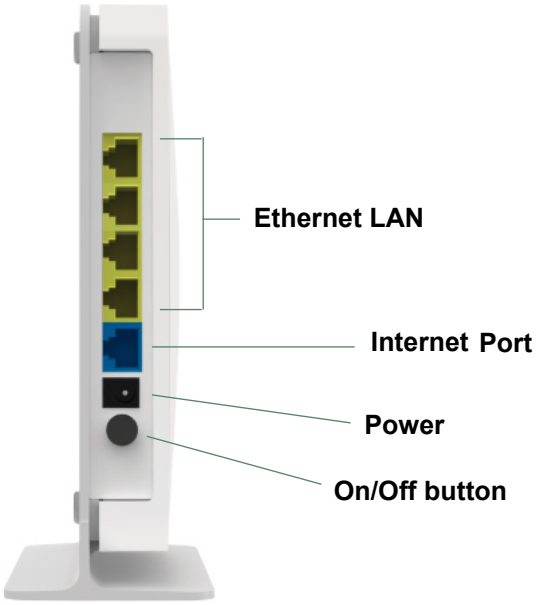


Figure 3. Router, rear view

See *Factory Default Settings* on page 96 for information about restoring factory settings.

Label

The label on the bottom of the router shows the WPS PIN, login information, MAC address, and serial number.

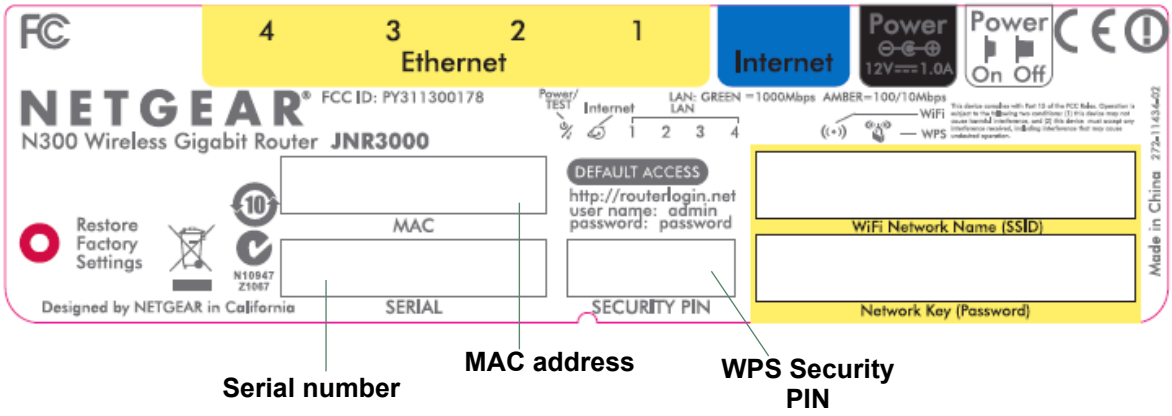


Figure 4. The label shows unique information about your router

2 Getting Started with NETGEAR Genie

Connecting to the router

This chapter explains how to use NETGEAR Genie to set up your router after you complete cabling as described in the installation guide and in the previous chapter in this book.

This chapter contains the following sections:

- *Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR Genie Setup*
- *Use NETGEAR Genie after Installation*
- *Upgrade Router Firmware*
- *Router Dashboard (Basic Home Screen)*
- *Add Wireless Devices or Computers to Your Network*

Router Setup Preparation

You can set up your router with the NETGEAR Genie automatically, or you can use the Genie menus and screens to set up your router manually. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, PCs, and other devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you need to change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP; this is rare)

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Router login** logs you in to the router interface from NETGEAR Genie. See *Use NETGEAR Genie after Installation* on page 17 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label located on the bottom of your router.

NETGEAR Genie Setup

NETGEAR Genie runs on any device with a web browser. It is the easiest way to set up the router because it automates many of the steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

➢ **To use NETGEAR Genie to set up your router:**

1. Turn the router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable (wired) or wirelessly (with the preset security settings listed on the bottom label) to your router.
3. Launch your Internet browser.
   - If this is the first time you are setting up the Internet connection for your router, the browser automatically goes to http://www.routerlogin.net, and the NETGEAR Genie screen displays.
   - If you already used the NETGEAR Genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR Genie screen. See *Use NETGEAR Genie after Installation* on page 17.
4. Follow the onscreen instructions to complete NETGEAR Genie setup. NETGEAR Genie guides you through connecting the router to the Internet.

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports, or wirelessly to the router.
- Make sure that the router has full power, and that the wireless LED is lit.
- Close and re-open the browser to make sure the browser does not cache the previous page.
- Browse to **http://www.routerlogin.net**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR Genie after Installation

When you first set up your router, NETGEAR Genie automatically starts when you launch an Internet browser on a computer that is connected to the router. You can use NETGEAR Genie again if you want to view or change settings for the router.

1. Launch your browser from a computer or wireless device that is connected to the router.
2. Type **http://www.routerlogin.net**.

   The login window displays:

3. Enter **admin** for the router user name and **password** for the router password, both in lowercase letters.

   Note: *The router user name and password are different from the user name and password for logging in to your Internet connection. See Types of Logins and Access on page 15 for more information.*

Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. See *Upgrade the Router Firmware* on page 53 for more information about upgrading firmware.

Click the message when it shows up, and click **Yes** to upgrade the router with the latest firmware. After the upgrade, the router restarts.

CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting and the Power LED has stopped blinking for several seconds.

Router Dashboard (Basic Home Screen)

The router Basic Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is an Advanced tab that is used to access additional menus and screens.

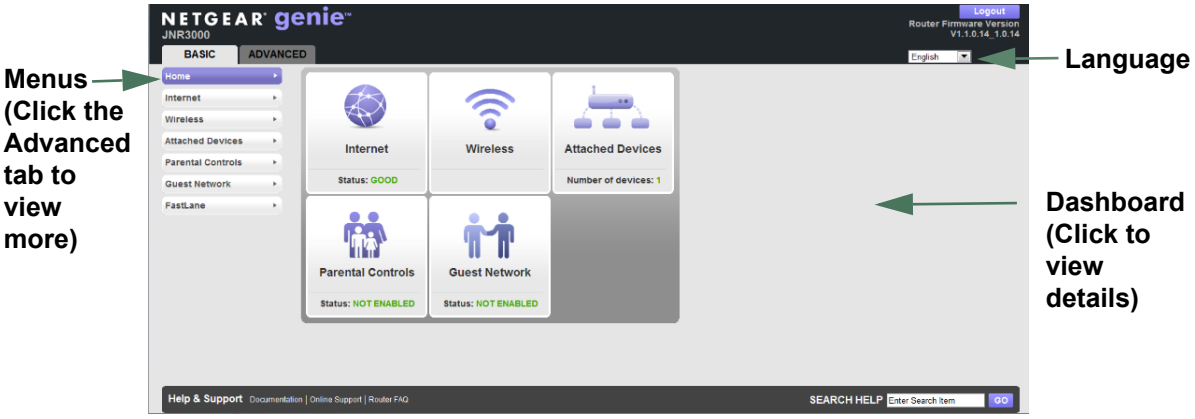


Figure 5. Router Basic Home screen with dashboard, language, and online help

- **Home**. This dashboard screen displays when you log in to the router.
- **Internet**. Set, update, and check the ISP settings of your router.
- **Wireless**. View or change the wireless settings for your router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.
- **Guest Network**. Set up a guest network to allow visitors to use your router's Internet connection.
- **FastLane**. Specify the bandwidth that you want reserved when you are connecting from a trusted IP address, and push the **FastLane** button. FastLane gives you guaranteed bandwidth for video streaming applications.
- **Advanced tab**. Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 7, Advanced Settings*. Using this tab requires a solid understanding of networking concepts.
- **Help & Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network. See *Guest Networks* on page 27 for instructions on how to set up a guest network.

Manual Method

➢ **To connect manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your router. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default Wi-Fi network name (SSID) and select it. The default SSID is located on the product label on the bottom of the router.
3. Enter the router password and click **Connect**. The default router passphrase is located on the product label on the bottom of the router.
4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard for easily adding computers and other devices to a home network while maintaining security. To use WPS, make sure that all wireless devices to be connected to the network are Wi-Fi certified and support WPS. During the connection process, the client gets the security settings from the router so that every device in the network has the same security settings.

➢ **To use WPS to join the wireless network:**

If your wireless device supports WPS (Push 'N' Connect), follow these steps:

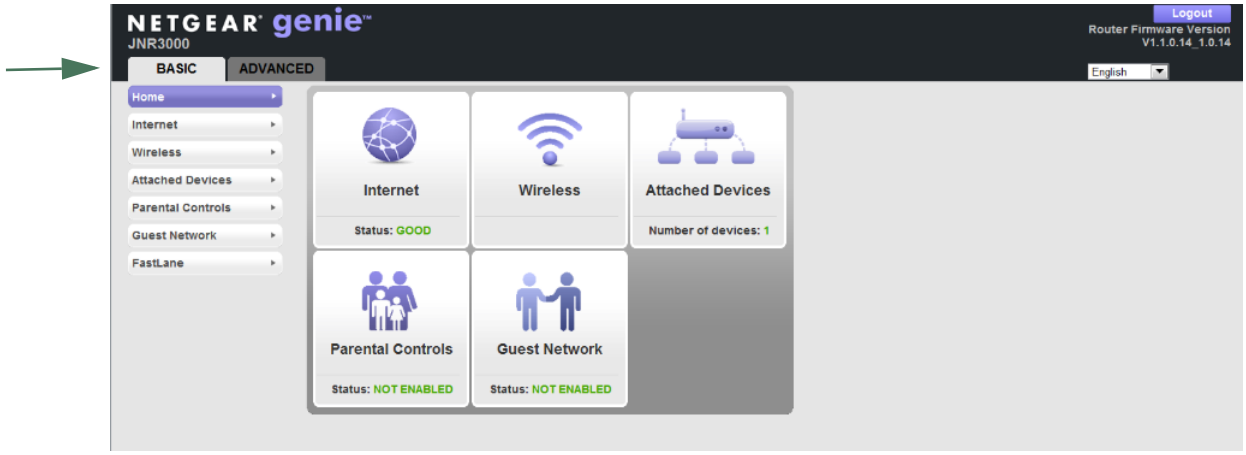
1. Press the **WPS** button on the router front panel .
2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device. The device is now connected to your router.
3. Repeat steps 1–2 to add other WPS wireless devices.

Genie Basic Settings

3

Your Internet connection and network

This chapter explains the features available from the Genie Basic Home screen, shown in the following figure:



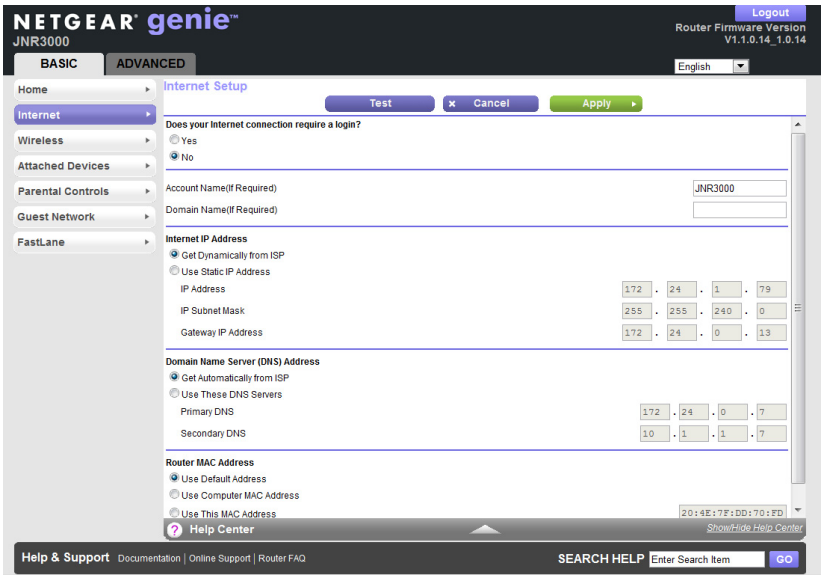
This chapter contains the following sections:

- *Internet Setup*
- *Attached Devices*
- *Parental Controls*
- *Basic Wireless Settings*
- *Guest Networks*
- *FastLane*

Internet Setup

The Internet Setup screen is where you view or change ISP information.

1. From the Home screen, select **Internet**. The following screen displays:



Scroll to view more settings

The fields that display in the Internet Setup screen depend on whether your Internet connection requires a login.

- **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
- **No**. Enter the account and domain names, only if needed.

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
3. Click **Apply** to save your settings.
4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 8, Troubleshooting*.

Internet Setup Screen Fields

The following descriptions explain all of the possible fields in the Internet Setup screen. The fields displayed on this screen depend on whether an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

These fields display when no login is required:

- **Account Name (If required)**. Enter the account name provided by your ISP. The Account Name is also called the host name.
- **Domain Name (If required)**. Enter the domain name provided by your ISP.

These fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation**. ISP types. The choices are PPPoE, PPTP, or L2TP.
- **Login**. The login name provided by your ISP. This is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **Idle Timeout (In minutes)**. If you want to change the login timeout, enter a new value in minutes. This value determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router will connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

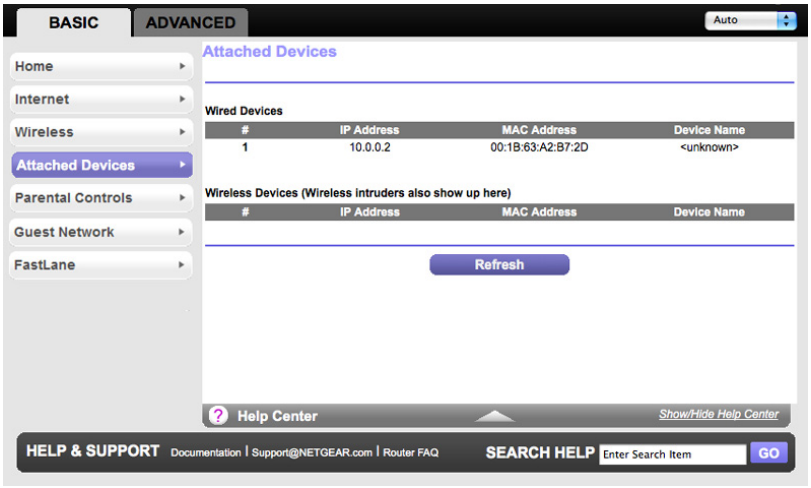
- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Router MAC Address. The Ethernet MAC address used by the router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (also called cloning).

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The router will capture and use the MAC address of the computer that you are now using. You have to use the one computer that is allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

Attached Devices

You can view all computers or devices that are currently connected to your network here. From the Basic Home screen, select **Attached Devices** to display the following screen:



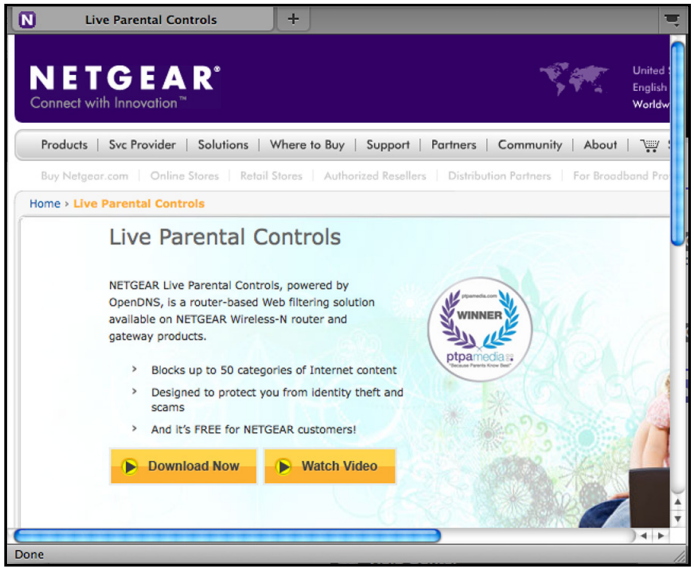
Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network.

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
- **Device Name**. If the device name is known, it is shown here.

You can click **Refresh** to update this screen.

Parental Controls

The first time you select Parental Controls from the Basic Home screen, you are automatically directed to the Internet, where you can learn more about Live Parental Controls or download the application. The following screen displays:



Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The JNR3000 router comes with preset security. This means that the Wi-Fi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

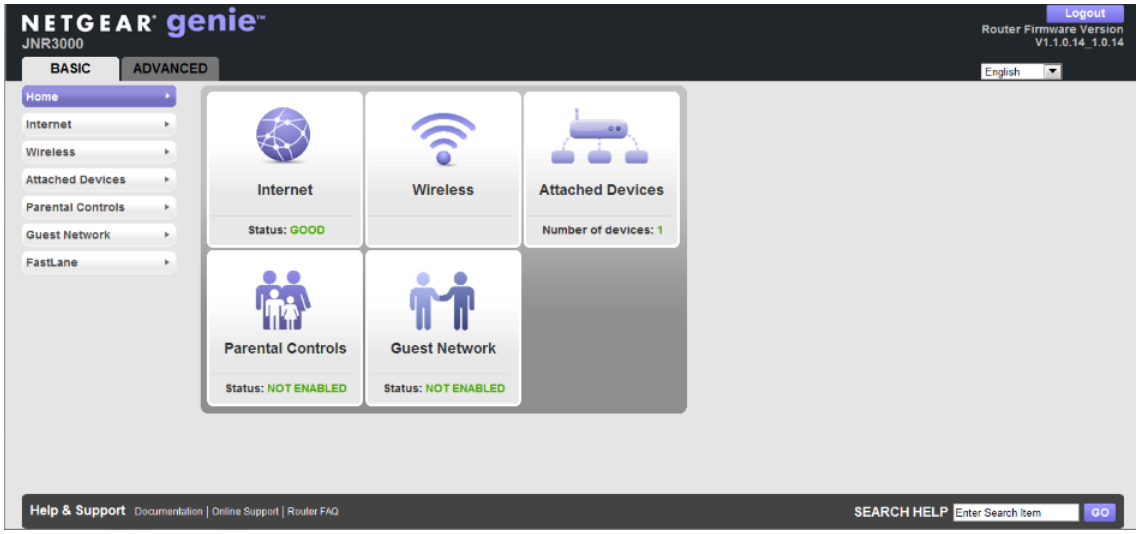
Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

➢ **To view or change basic wireless settings:**

NETGEAR recommends that you do not change your preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click **Apply**. To avoid this problem, use a computer with a wired connection to access the router.

1. On the Basic Home screen, select **Wireless** to display the Wireless Settings screen.



   The screen sections, settings, and procedures are explained in the following sections.

2. Make any needed changes, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
   - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
   - Does your wireless device or computer show up on the Attached Devices screen? If it does, then it is connected to the network.
   - If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your router.

Wireless Settings Screen Fields

Region Selection

The location where the router is used. Select from the countries in the list. Note that in the United States, the region is fixed to United States and is not changeable.

Wireless Network

Enable SSID Broadcast. This setting allows the router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box, and click **Apply**.

Enable Wireless Isolation. If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Enable NETGEAR Badge LED. This setting lets you enable the NETGEAR Badge LED.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and ***NETGEAR strongly recommends that you do not change this setting.***

Channel. This setting is the wireless channel used by the gateway. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

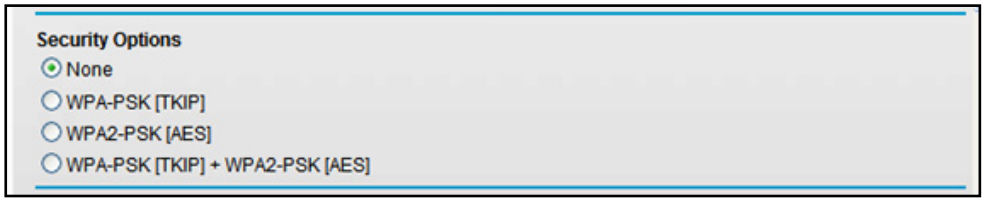
Mode. Up to 300 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 450 Mbps setting allows 802.11n devices to connect at this speed.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. ***NETGEAR recommends that you do not change the security option or passphrase****,* but if you want to change these settings, this section explains how. ***Do not disable security***.

Change WPA Security Option and Passphrase

1. Under Security Options, select the WPA option you want.



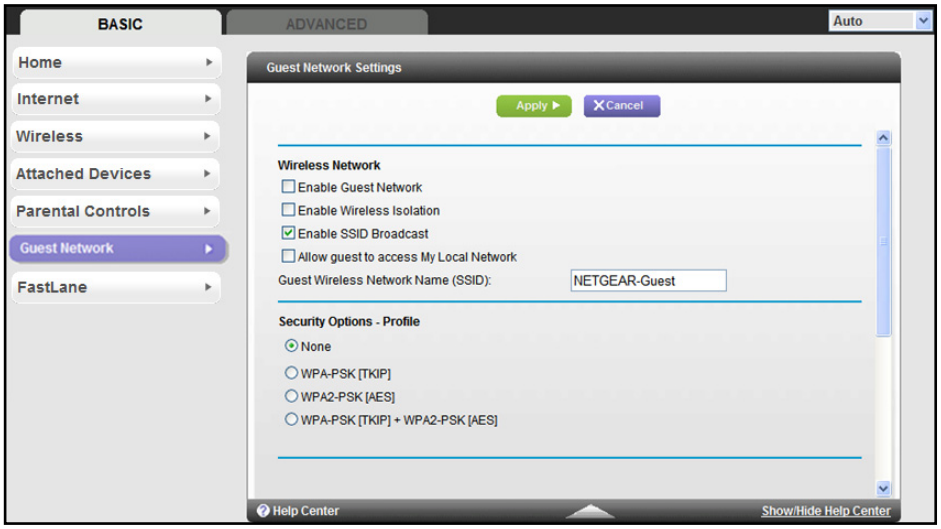
2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Guest Networks

Adding a guest network allows visitors at your home to use the Internet without giving them your wireless security key.

➢ **To set up a guest network:**

1. Select **Basic > Guest Network** to display the following screen:



2. Select any of the following wireless settings:

   Enable Guest Network. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.

   Enable Wireless Isolation. If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

   Enable SSID Broadcast. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.

   Allow guest to access My Local Network. If this check box is selected, any user who connects to this SSID has access to your local network, not just Internet access.

3. Give the guest network a name.

   The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main non-guest SSID.

4. Select a security option from the list. The security options are described in *Guest Network Wireless Security Options* on page 28.

5. Click **Apply** to save your selections.

Guest Network Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. Wi-Fi Protected Access (WPA) has several options including pre-shared key (PSK) encryption.

This section presents an overview of the security options and provides guidance on when to use which option. It is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend this.

WPA Encryption

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA uses a passphrase to perform authentication and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.

WPA2-PSK is stronger than WPA-PSK. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is usually implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring their WPA settings.

FastLane

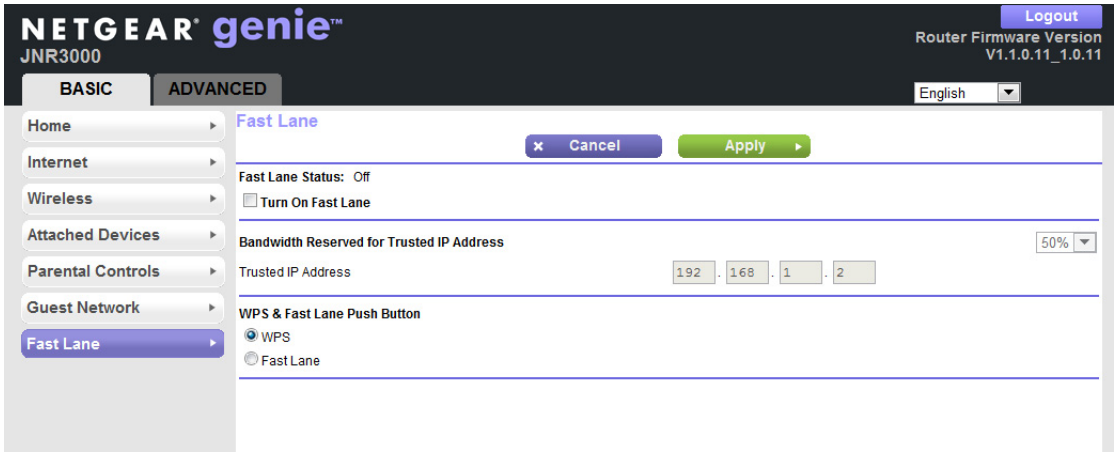
FastLane lets you specify the bandwidth that you want reserved when you are connecting from a trusted IP address, and push the **FastLane** button. FastLane gives you guaranteed bandwidth for video streaming applications.

From the Basic screen, you can:

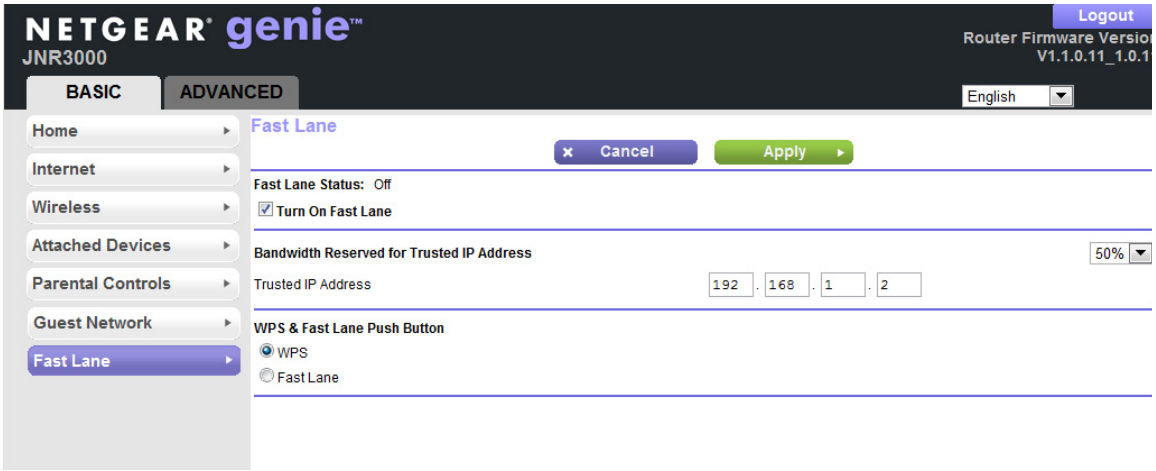
- Turn the FastLane feature on and off. (FastLane is set to off by default.)
- Specify the amount of bandwidth reserved for the trusted IP address.
- Set the WPS/FastLane button on your router to WPS or FastLane. (This button is set to WPS by default.)

To use FastLane:

1. Select **FastLane** from the Basic screen menu. The first FastLane screen appears:



2. To select FastLane features, set the screen like this:



- **FastLane Status**: By default, FastLane is turned off, and WPS is turned on. To turn on FastLane, check the **Turn On FastLane** check box.

- **Bandwidth Reserved for Trusted IP Address**: Specify the percentage of bandwidth on the wireless router to reserve when you connect from a trusted IP address. This prevents other users from using up your bandwidth. When you connect to the router from the trusted IP address, you have guaranteed bandwidth for video streaming applications.
  - Enter the IP address in the fields provided.
  - Select a percentage from the drop-down list: 50%, 60%, 70%, or 80%.
- **WPS and FastLane Push Button**: Select **FastLane** by clicking the FastLane radio button.

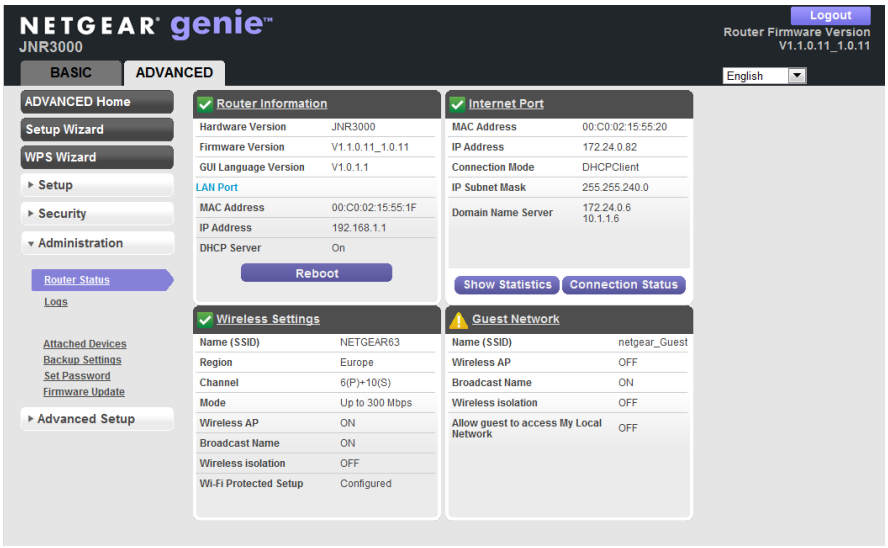
3. Click **Apply** to save your changes.

Genie Advanced Home

4

Specifying custom settings

This chapter explains the features available from the Genie Advanced Home screen, shown in the following figure:



This chapter contains the following sections:

- *Setup Wizard*
- *WPS Wizard*
- *Setup Menu*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

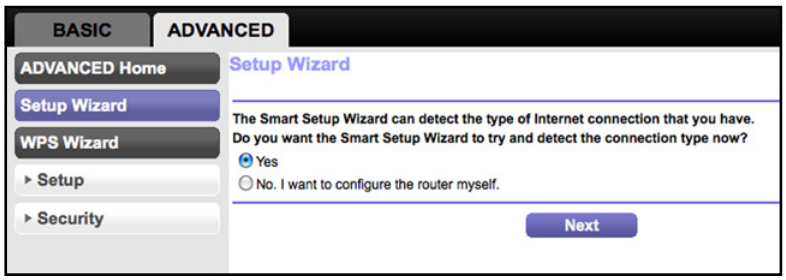
Some selections on the Advanced Home screen are described in separate chapters:

- **Security**. See *Chapter 5, Security*.
- **Administration**. See *Chapter 6, Administration*.
- **Advanced Setup**. See *Chapter 7, Advanced Settings*.

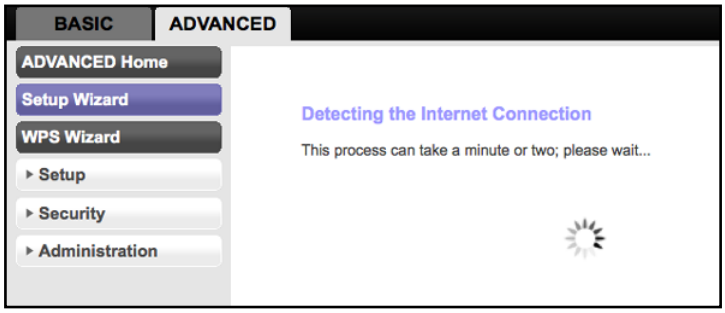
Setup Wizard

The NETGEAR Genie installation process is launched the first time you set up the router. After setting up the router the first time, if you want to perform this task again, you can run Setup Wizard from the Advanced tab of the Genie.

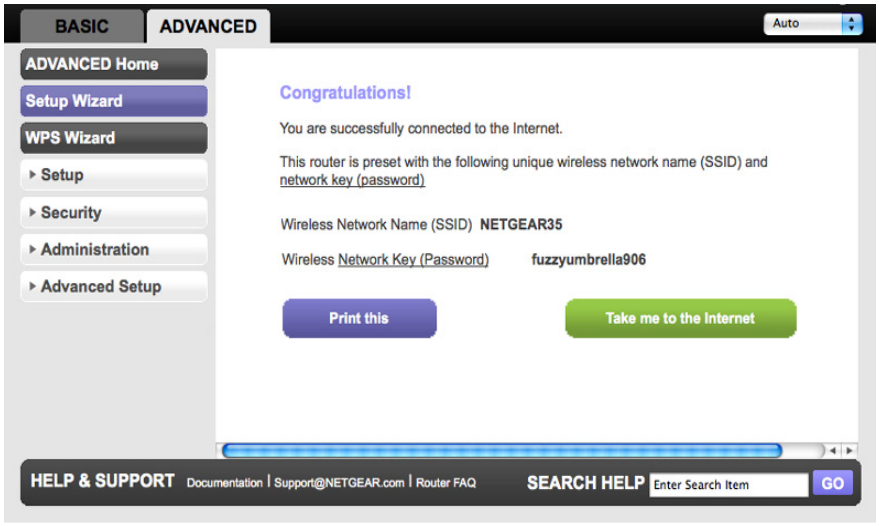
1. Select **Setup Wizard** to display the following screen:



2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, you are taken to the Internet Setup screen (see *Internet Setup* on page 21).
3. If you selected Yes, click **Next**. The following screen displays:



The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. The following screen displays:

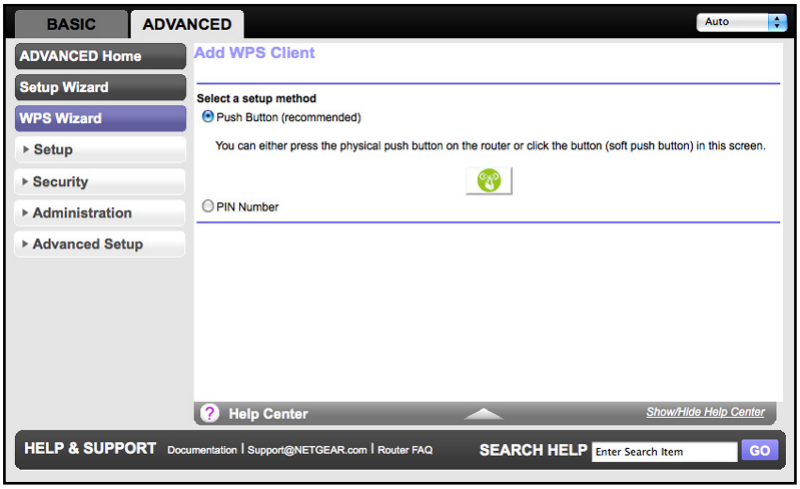


WPS Wizard

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device, you need to press the WPS button or locate its WPS PIN.

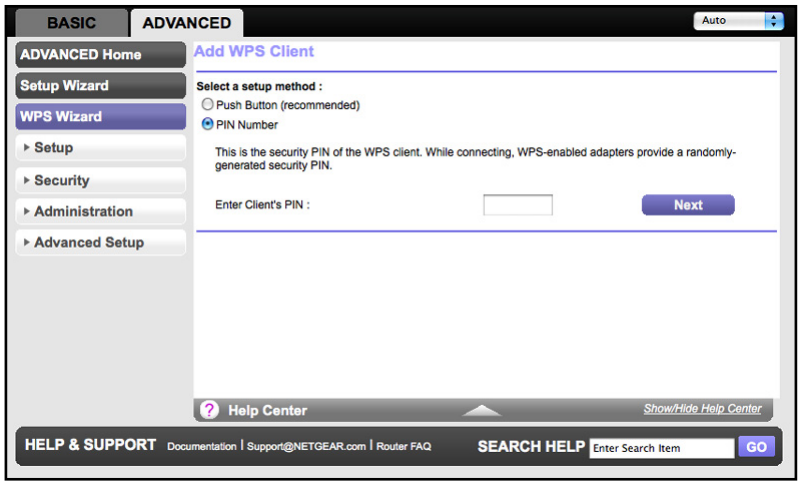
To use the WPS Wizard:

1. Select **Advanced > WPS Wizard**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).



You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.
   - To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button located on the side of the router. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
   - To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.



Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

The router attempts to add the WPS-capable device. The WPS LED on the front of the router blinks green. When the router establishes a WPS connection, the LED is solid green, and the router WPS screen displays a confirmation message.

4. Repeat Step 2 and Step 3 to add another WPS client to your network.

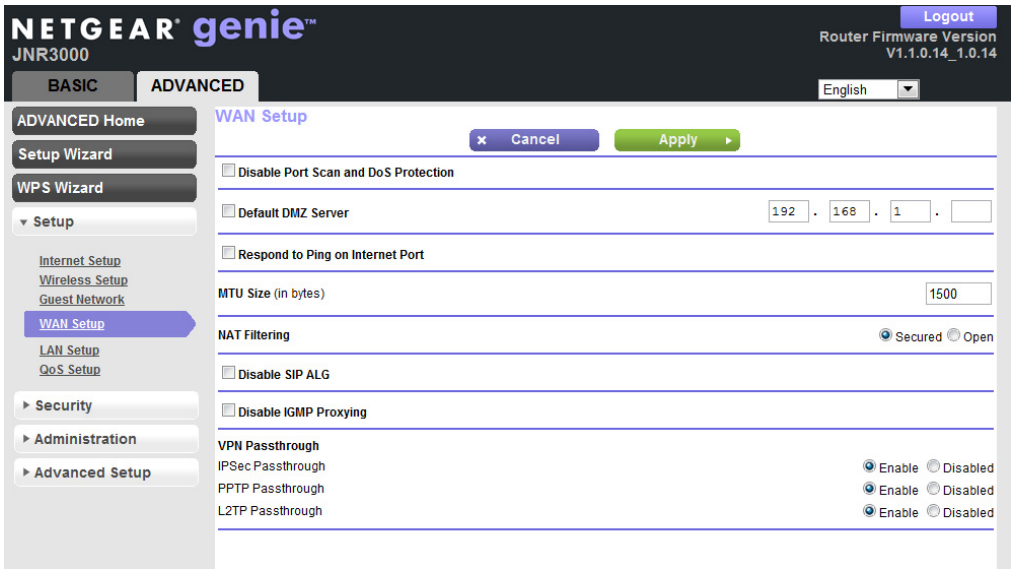
Setup Menu

Select **Advanced > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup**. This is a shortcut to the same Internet Setup screen that you can access from the dashboard on the Basic Home screen. See *Internet Setup* on page 21.
- **Wireless Setup**. This is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the Basic Home screen. See *Basic Wireless Settings* on page 24.
- **Guest Network**. This is a shortcut to the same Guest Network screen that you can access from the dashboard on the Basic Home screen. See *Guest Networks* on page 27.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 35.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 38.
- **QoS Setup**.Quality of Service (QoS) setup. See *Quality of Service (QoS) Setup* on page 41.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the router to respond to a ping on the WAN (Internet) port. Select **Advanced > Setup > WAN Setup** to view the following screen:



- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This option should be disabled only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the router to respond to a ping from the Internet, select this check box. Use this option only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. You can select this check box to disable the feature if you do not need it.
- **MTU Size (in bytes)**. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. See *Change the MTU Size* on page 36.
- **NAT Filtering**. Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT

provides a much less secured firewall, but allows almost all Internet applications to function.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

WARNING!

DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

Incoming traffic from the Internet is usually discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets have to be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that will not open, or displays only part of a web page

  - Yahoo email
  - MSN portal
  - America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems, such as the inability to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ **To change the MTU size:**

1. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size between 64 and 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The router's default LAN IP configuration is:

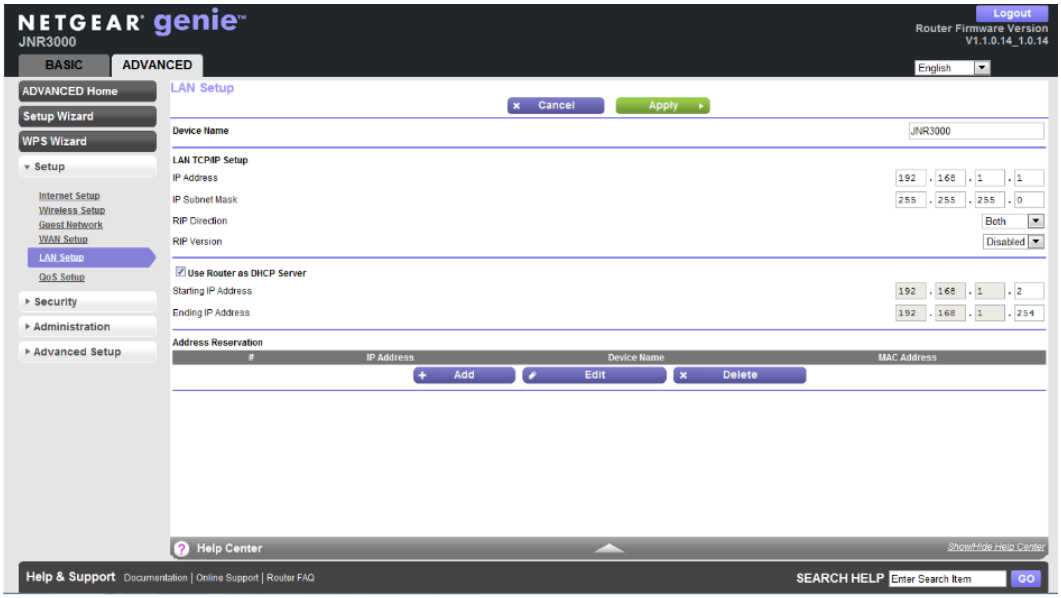
- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network requires that you use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

➢ **To change the LAN settings:**

> **Note:** If you change the LAN IP address of the router while connected through the browser, you are disconnected, and will have to open a new connection to the new IP address and log in again.

1. Select **Advanced > Setup > LAN Setup** to display the following screen:



2. Enter the settings that you want to customize. These settings are described in the following section, *LAN Setup Screen Settings*.
3. Click **Apply** to save your changes.

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or router.
- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **RIP Version**. This option controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.

  RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup.

  RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

Use Router as a DHCP Server

This check box is usually selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Use the Router as a DHCP Server

By default, the router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Internet Setup screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Setup screen)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as 192.168.1.x.)
3. Type the MAC address of the computer or server.

   Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

   The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The JNR3000 router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

Select **Advanced > Setup > QoS Setup** to display the following screen:

Enable WMM QoS for Wireless Multimedia Applications

The JNR3000 router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific device by MAC address

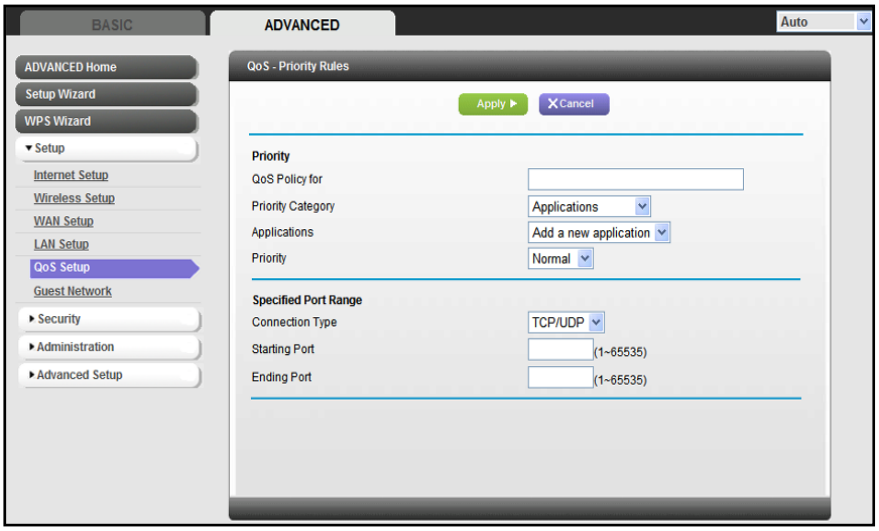
To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

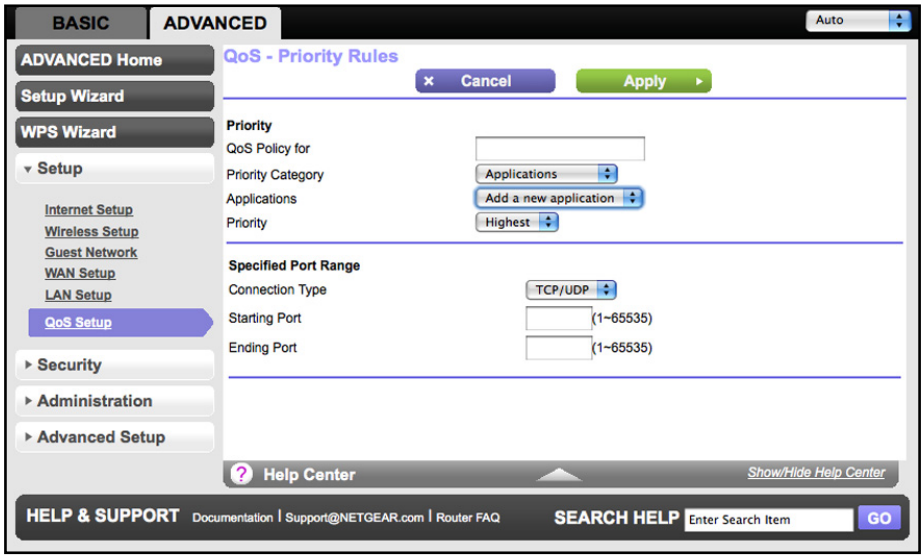
1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button to see the existing priority rules. On this screen, you can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all of the rules by simply clicking the **Delete All** button.

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:



4. In the QoS Policy for field, type the name of the application or game.
5. In the Priority Category list, select either **Applications** or **Online Gaming**. In either case, a list of applications or games displays in the list.
6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.

a. If you add a new entry, the Priority Rules screen expands as shown:



b. In the QoS Policy for field, enter a descriptive name for the new application or game.

c. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.

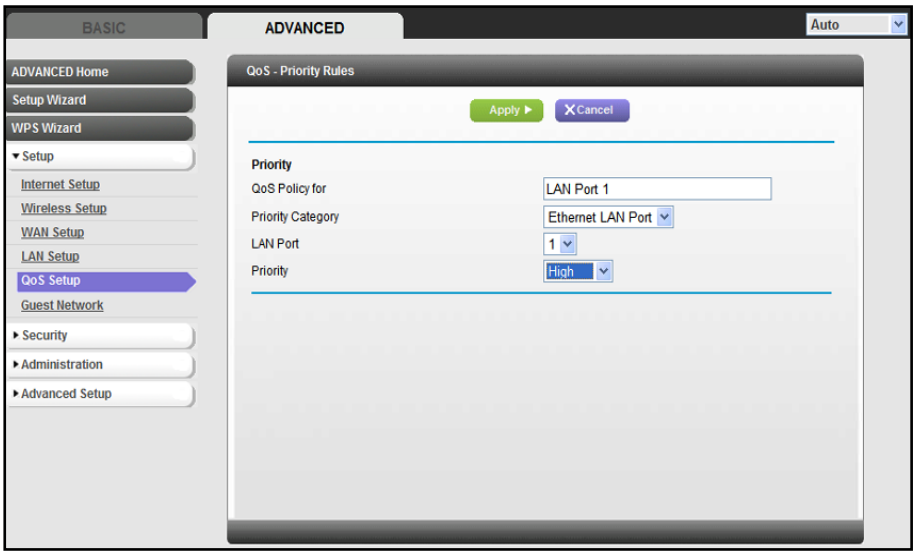
7. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a Router LAN Port

➢ **To create a QoS policy for a device connected to one of the router's LAN ports:**

1. Select **Advanced > Setup > QoS Setup** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button.
3. Click the **Add Priority Rule** button.

4. From the Priority Category list, select **Ethernet LAN Port**, as shown in the following figure:



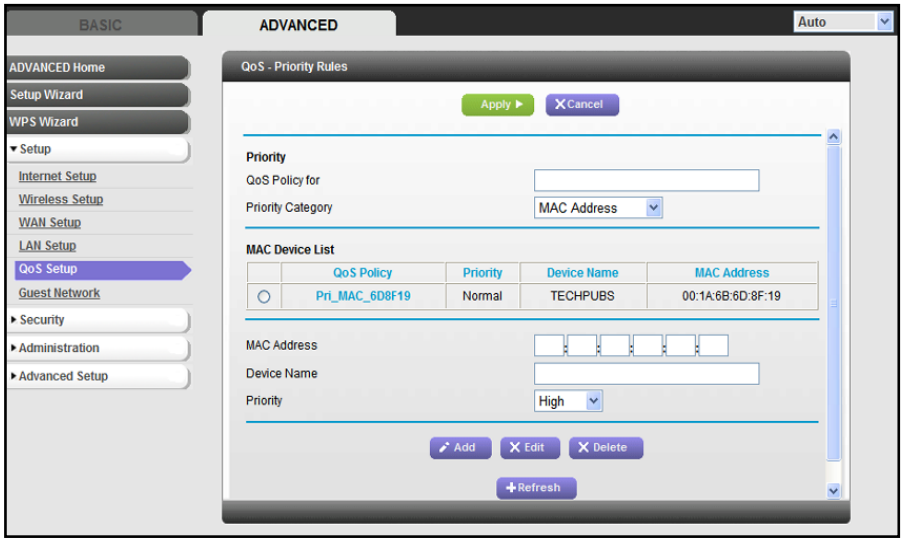
5. From the LAN port list, select the LAN port that will have a QoS policy.
6. From the Priority list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **Advanced > Setup > QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays.
2. Click **Add Priority Rule**.

3. From the Priority Category list, select **MAC Address** to display the following screen:



4. If the device to be prioritized appears in the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you have to complete these fields manually.
5. From the Priority list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Editing or Deleting an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **Advanced > QoS Setup** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply** in the QoS Setup screen to save your changes.

Security

Keeping unwanted content out of your network

5

This chapter explains how to use the basic firewall features of the router to prevent objectionable content from reaching the PCs and other devices connected to your network.

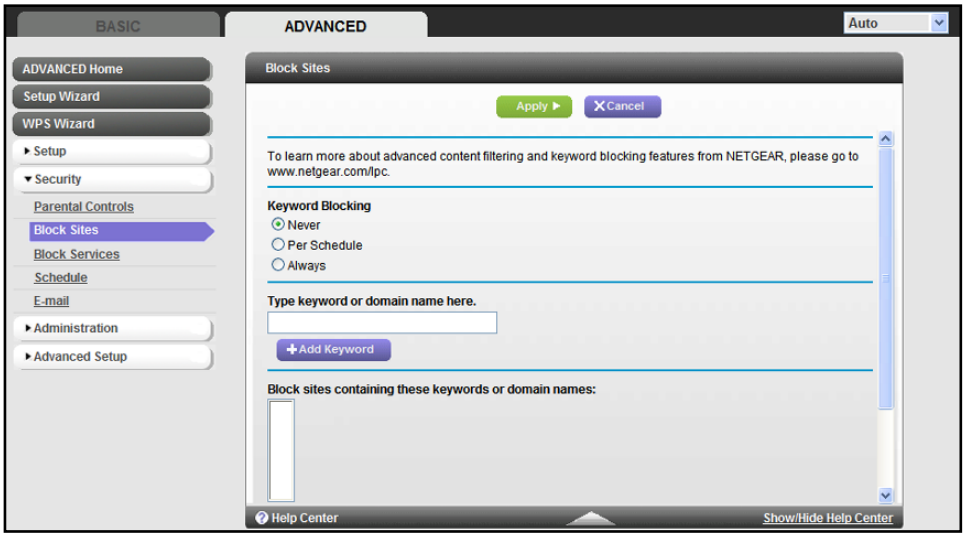
This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Schedule Blocking*
- *Security Event Email Notifications*

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

1. Select **Advanced > Security > Block Sites** to display the following screen:



2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (.) to block all Internet browsing access.

➢ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword**, and then **Apply** to save your changes.

➢ **To specify a trusted computer:**

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

Block Services (Port Filtering)

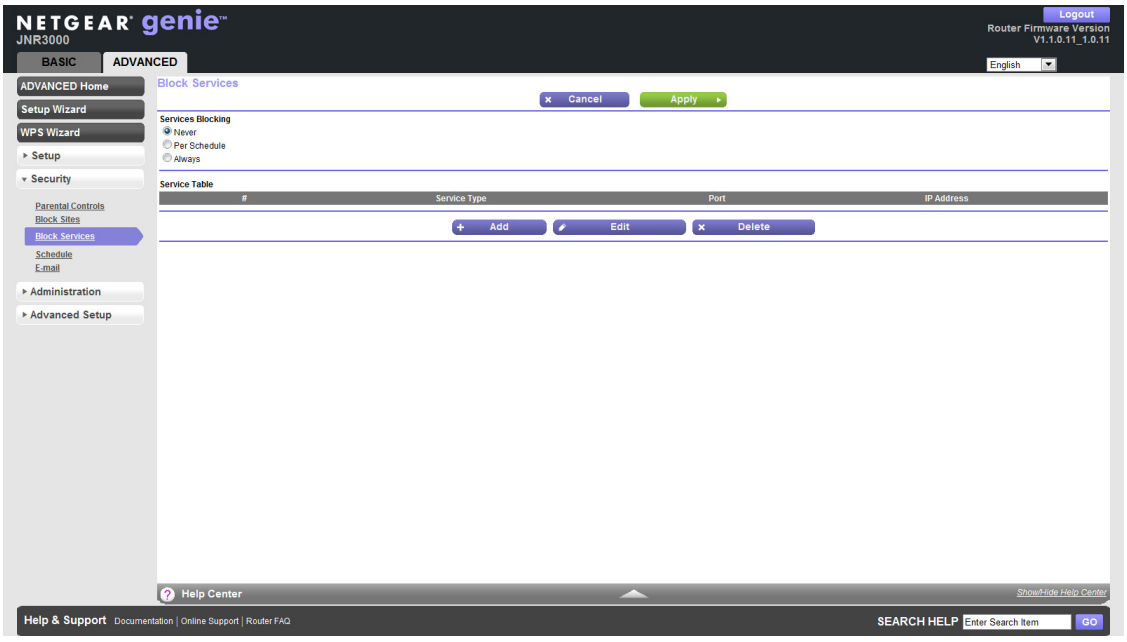
Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers are used by the application.

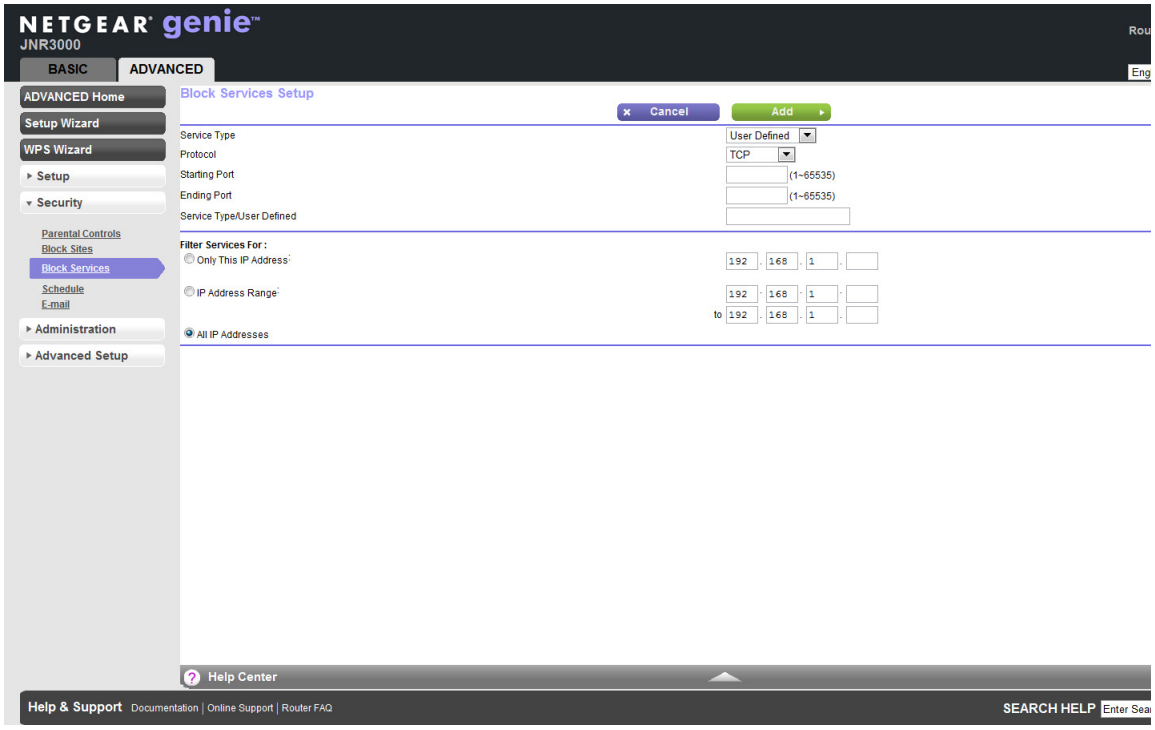
➢ **To block services:**

1. Select **Advanced > Security > Block Services** to display the following screen:



2. Select either **Per Schedule** or **Always** to enable service blocking, and click **Apply**. If you selected Per Schedule, specify a time period in the Schedule screen as described in *Schedule Blocking* on page 50.

3. Click **Add** to add a service. The Block Services Setup screen displays:



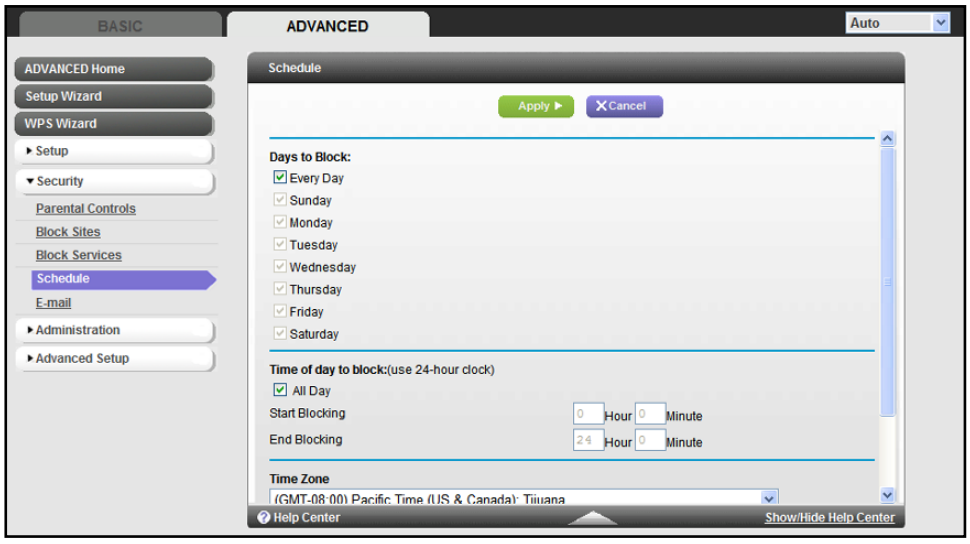
4. From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined.**
5. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
6. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
7. Select the radio button for the IP address configuration you want to block, and enter the IP addresses. You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.
8. Click **Add** to enable your Block Services Setup selections.

Schedule Blocking

You can specify the days and time that you want to block Internet access.

➢ **To schedule blocking:**

1. Select **Advanced > Security > Schedule** to display the following screen:



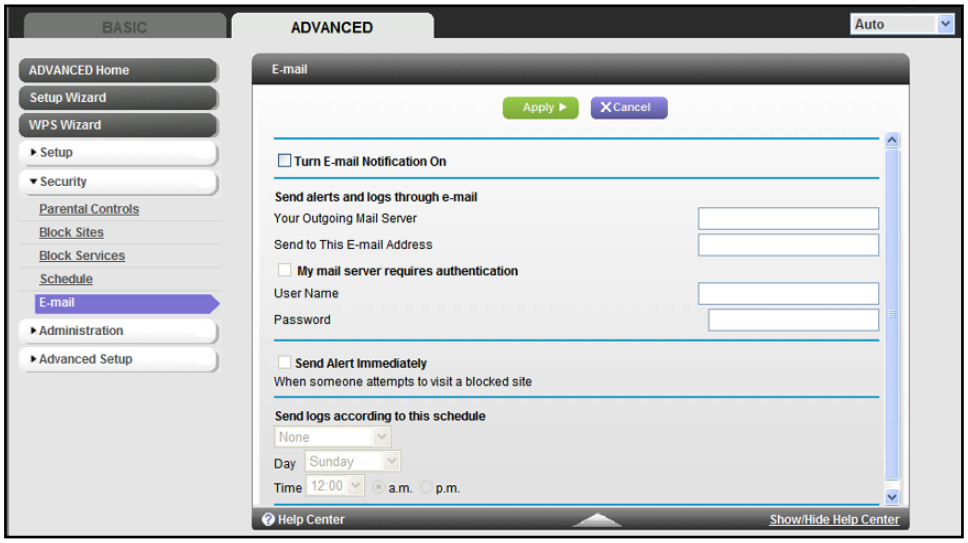
2. Set up the schedule for blocking keywords and services.
   - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.
3. Select your time zone from the list. If you use daylight savings time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply** to save your settings.

Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the Email screen, and specify which alerts you want to receive and how often.

➢ **To set up email notifications:**

1. Select **Advanced > Security > Email** to display the following screen:



2. To receive email logs and alerts from the router, select the **Turn Email Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent by email.
4. Enter the email address to which logs and alerts are sent in the Send to This Email Address field. This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent by email.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. You can have email alerts sent immediately when someone attempts to visit a blocked site, and you can specify that logs are sent automatically.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, the log is cleared from the router's memory. If the router cannot email the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.
7. Click **Apply** to save your settings.

Administration

6

Managing your network

This chapter describes the router settings for administering and maintaining your router and home network. See also *Remote Management* on page 81 for information about upgrading or checking the status of your router over the Internet, and *Traffic Meter* on page 83 for information about monitoring the volume of Internet traffic passing through your router's Internet port.

This chapter includes the following sections:

- *Upgrade the Router Firmware*
- *View Router Status*
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Set Password*

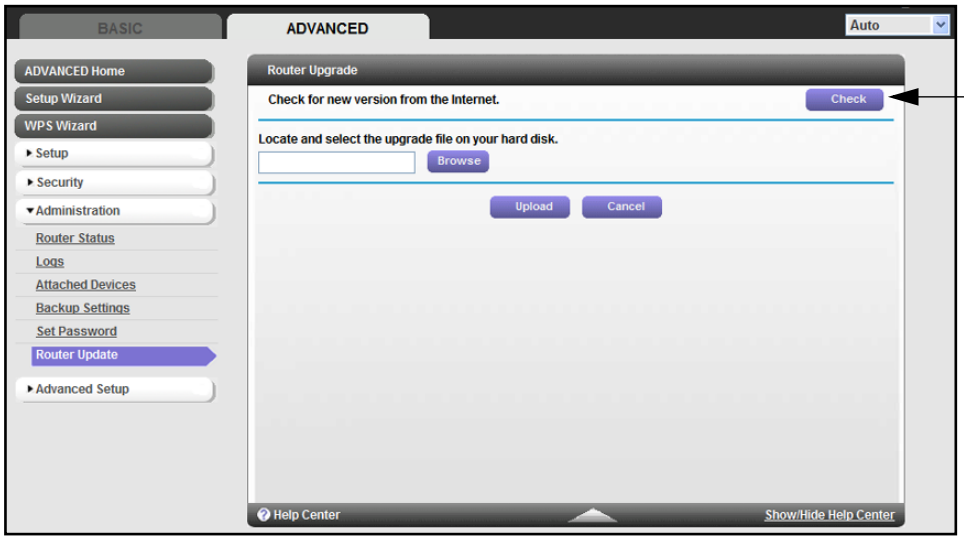
Upgrade the Router Firmware

The router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the Advanced tab. You might see a message at the top of the Genie screens when new firmware is available for your product.

You can use the **Check** button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

➢ **To check for new firmware and update your router:**

1. Select **Advanced > Administration > Router Update** to display the following screen:



2. Click **Check**.

   The router finds new firmware information if any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).

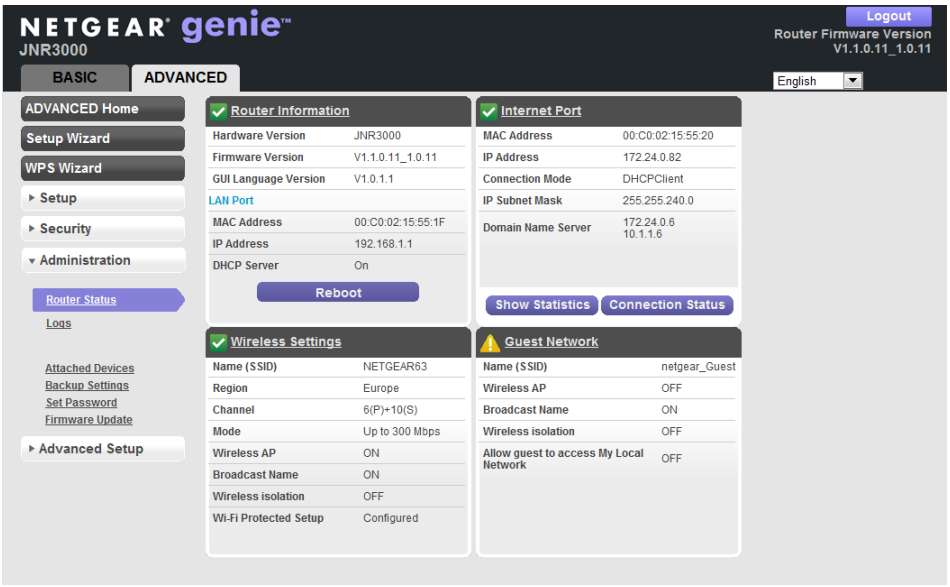
WARNING!

When uploading firmware to the router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether you need to reconfigure the router after upgrading.

View Router Status

To view router status and usage information, select **Advanced Home** or select **Administration > Router Status** to display the following screen:



Router Information

Hardware Version. The router model.

Firmware Version. The version of the router firmware. It changes if you upgrade the router firmware.

GUI Language Version. The localized language of the user interface.

LAN Port.

- **MAC Address**. The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the router.
- **IP Address**. The IP address being used by the Ethernet (LAN) port of the router. The default is 192.168.1.1.
- **DHCP Server**. Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.

Internet Provider (WAN) Setup

MAC Address. The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the router.

IP Address. The IP address being used by the Internet (WAN) port of the router. If no address is shown or the address is 0.0.0, the router cannot connect to the Internet.

Connection. This shows if the router is using a fixed IP address on the WAN. If the value is DHCP Client, the router obtains an IP address dynamically from the ISP.

IP Subnet Mask. The IP subnet mask being used by the Internet (WAN) port of the router.

Domain Name Server. The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as *www.netgear.com* into IP addresses.

Statistics Button

On the Router Status screen, in the Internet Provider (WAN) Setup pane, click the **Statistics** button to display the following screen:

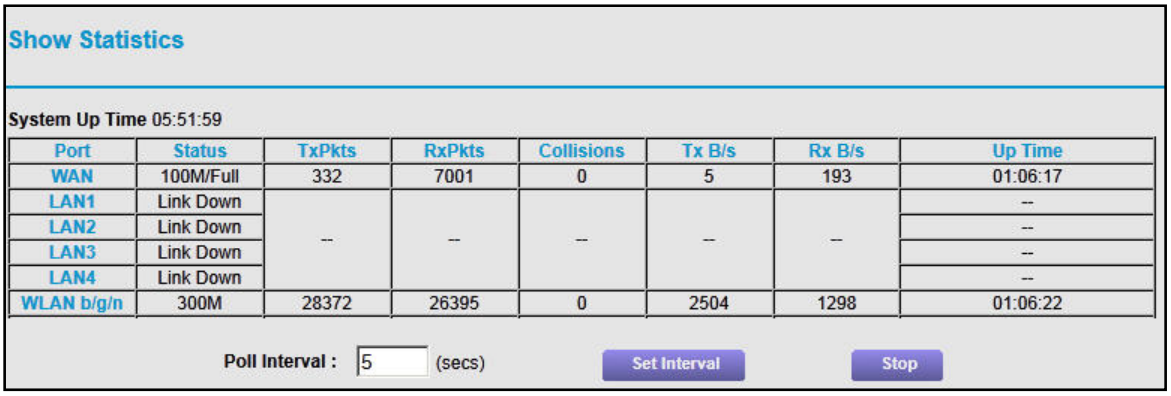


Figure 6. System up time and poll interval statistics

System Up Time. The time elapsed since the router was last restarted.

Port. The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted on this port since reset or manual clear.
- **RxPkts**. The number of packets received on this port since reset or manual clear.
- **Collisions**. The number of collisions on this port since reset or manual clear.
- **Tx B/s**. The current transmission (outbound) bandwidth used on the WAN and LAN ports.
- **Rx B/s**. The current reception (inbound) bandwidth used on the WAN and LAN ports.
- **Up Time**. The time elapsed since this port acquired the link.
- **Poll Interval**. The interval at which the statistics are updated in this screen.

To change the polling frequency, enter a time in seconds in the Poll Interval field, and click **Set Interval**.

To stop the polling entirely, click **Stop**.

Connection Status Button

On the Router Status screen in the Internet Connection pane, click the **Connection Status** button to view connection status information.

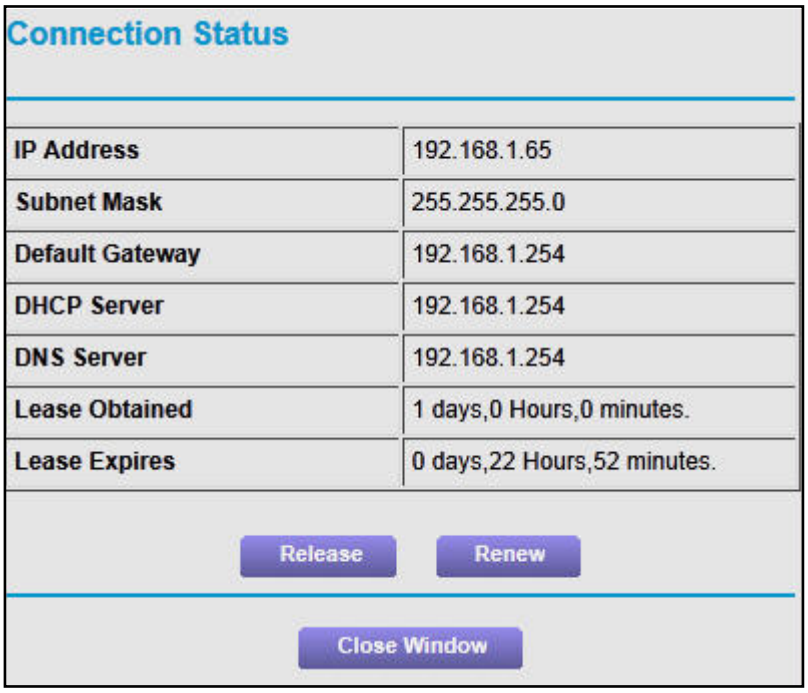


Figure 7. View connection status information

The Release button returns the status of all items to 0. The Renew button refreshes the items. The Close Window button closes the Connection Status screen.

IP Address. The IP address that is assigned to the router.

Subnet Mask. The subnet mask that is assigned to the router.

Default Gateway. The IP address for the default gateway that the router communicates with.

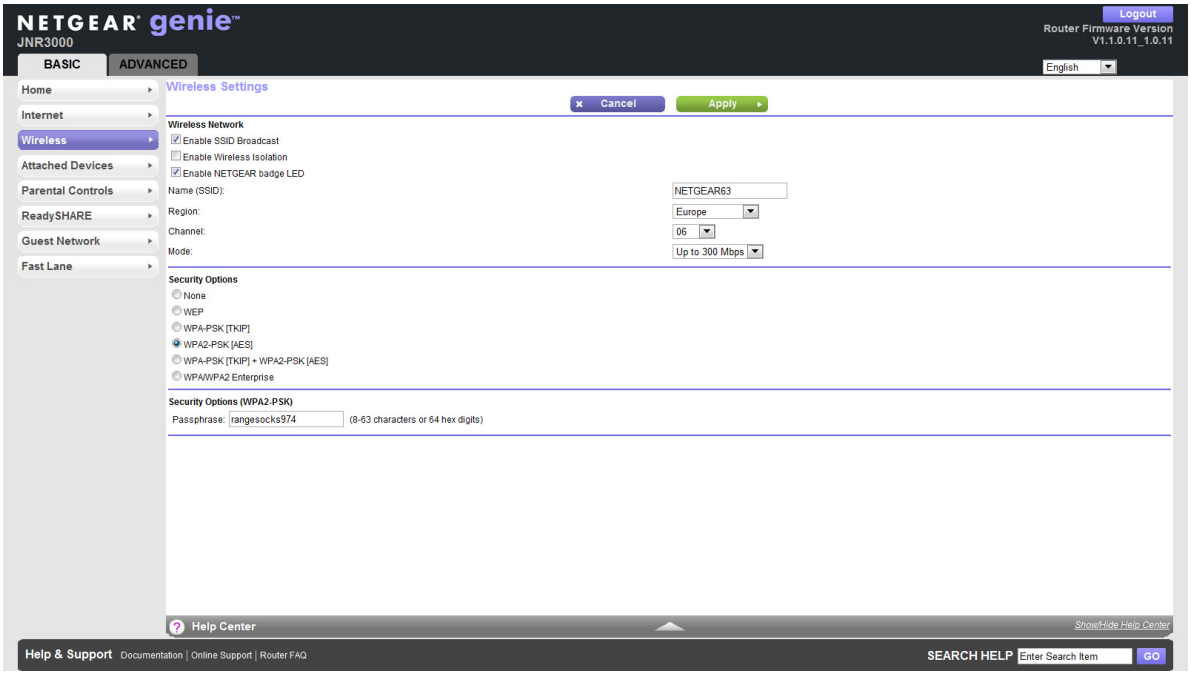
DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.

DNS Server. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

Lease Obtained. The date and time when the lease was obtained.

Lease Expires. The date and time that the lease expires.

Wireless Settings



The following settings are displayed:

Name (SSID). The wireless network name (SSID) used by the router.

Region. The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.

Channel. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the router finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 will not interfere with each other.

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 217 Mbps (default), and Up to 450 Mbps.

Wireless AP. Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the router is broadcasting its SSID.

Wireless Isolation. Select this check box only if you want to prevent wireless connections to the router.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

Guest Network

Name (SSID). The 11N wireless network name (SSID) used by the router. The default names are NETGEAR-Guest and NETGEAR-5G-Guest.

Wireless AP. Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the router is broadcasting its SSID.

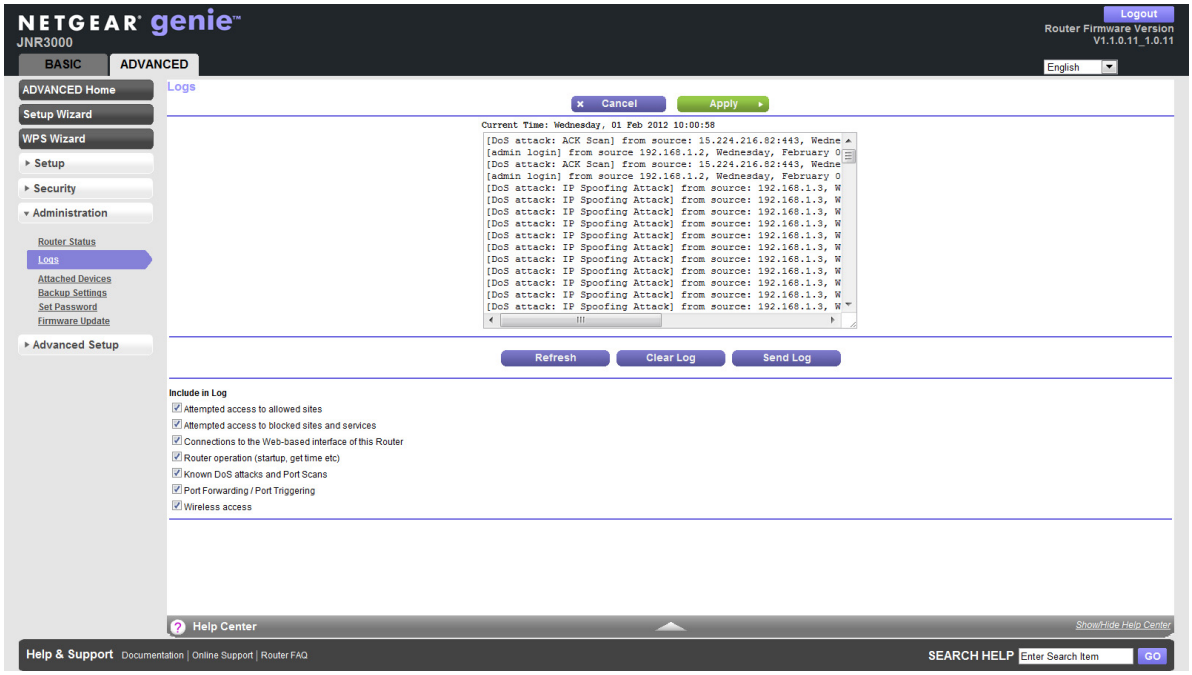
Wireless Isolation. Select this check box only if you want to prevent wireless connections to the router.

Allow guest to access My Local Network. If selected, any user who connects to this SSID can access local networks associated with the router.

View Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **Advanced > Administration > Logs**. The Logs screen displays.



The log screen shows the following information:

- **Date and time**. The date and time the log entry was recorded.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Target address**. The name or IP address of the website or news group visited or to which access was attempted.
- **Action**. Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button.

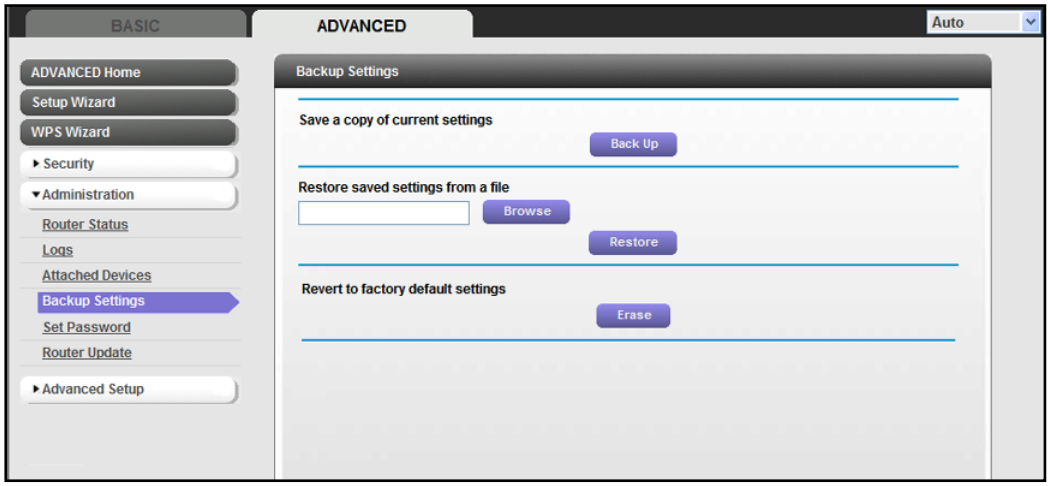
Manage the Configuration File

The configuration settings of the JNR3000 router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➢ **To back up the router's configuration settings:**

1. Select **Advanced > Administration > Backup Settings** to display the following screen:



2. Click **Back Up** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

➢ **To restore configuration settings that you backed up:**

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the router.

Upon completion, the router reboots.

WARNING!

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings.

You can either use the Restore Factory Settings button on the back of the router (see *Factory Default Settings* on page 96), or you can click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the router's DHCP.

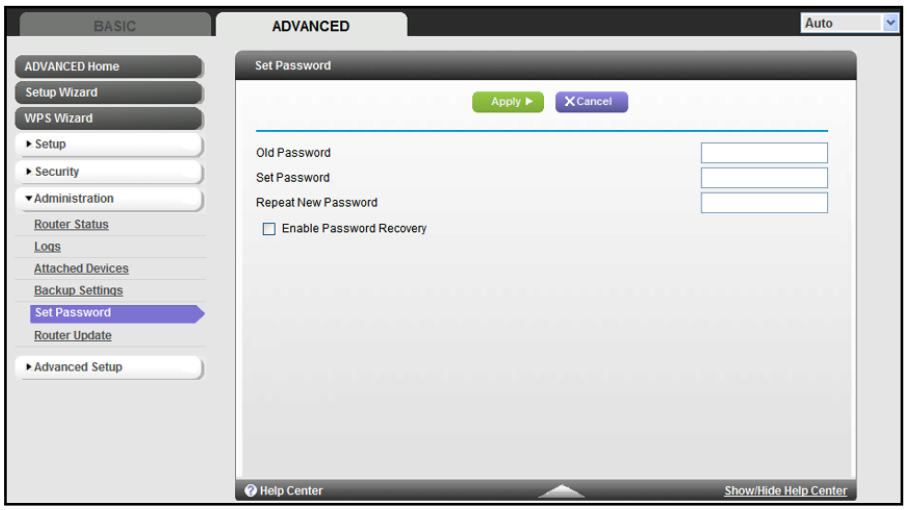
Set Password

This feature allows you to change the default password that is used to log in to the router with the user name **admin**.

Changing the default password is not the same as changing the password for wireless access. The label on the bottom of your router shows your unique wireless network name (SSID) and password for wireless access (see *Label* on page 13).

➢ **To set the password for the user name admin:**

1. Select **Advanced > Administration > Set Password** to display the following screen:



2. Type the old password, and type the new password twice in the fields on this screen.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.
4. Click **Apply** so that your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the default password. Then you have an easy way to recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.
3. Click **Apply** to save your changes.

When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Advanced Settings

7

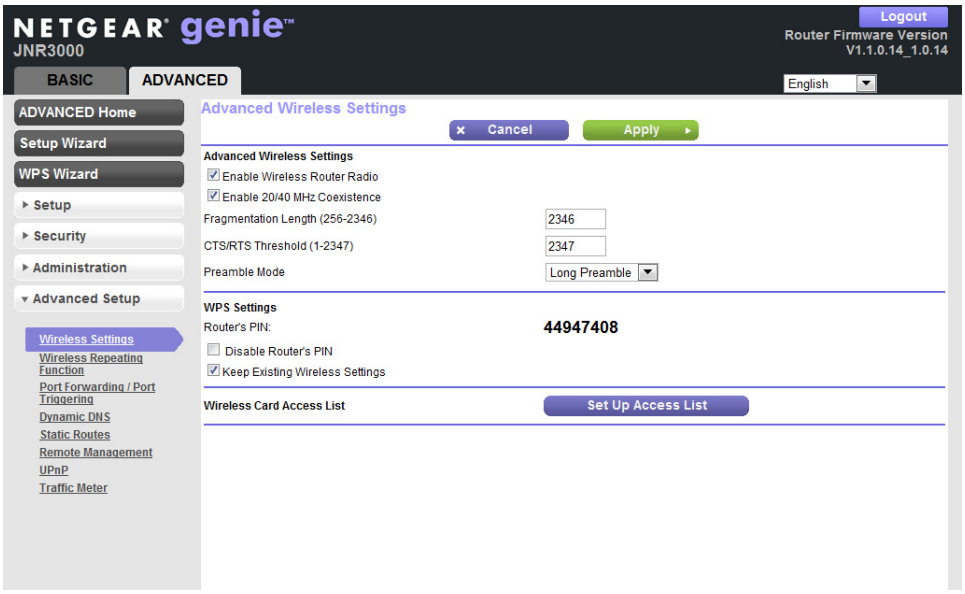
This chapter describes the advanced features of your router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Repeating Function (WDS)*
- *Port Forwarding and Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *Traffic Meter*

Advanced Wireless Settings

Select **Advanced > Advanced Setup > Wireless Settings** to display the following screen:



The following settings are available in this screen:

Enable Wireless Router Radio. You can completely turn off the wireless portion of the wireless router by clearing this check box. Select this check box again to enable the wireless portion of the router. When the wireless radio is disabled, other members of your household can use the router by connecting their computers to the router with an Ethernet cable.

Note: The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Turn off wireless signal by schedule. You can use this feature to turn off the wireless signal from your router at times when you do not need a wireless connection. For instance, you could turn it off for the weekend if you leave town.

WPS Settings.You can add WPS devices to your network.

Wireless Card Access List. Click the **Set Up Access List** button display the Wireless Card Access List screen. On this screen you can restrict access to your network to specific devices based on their MAC address.

Wireless Repeating Function (WDS)

You can set the JNR3000 router up to be used as a wireless access point (AP). Doing this enables the router to act as a wireless repeater. A wireless repeater connects to another wireless router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

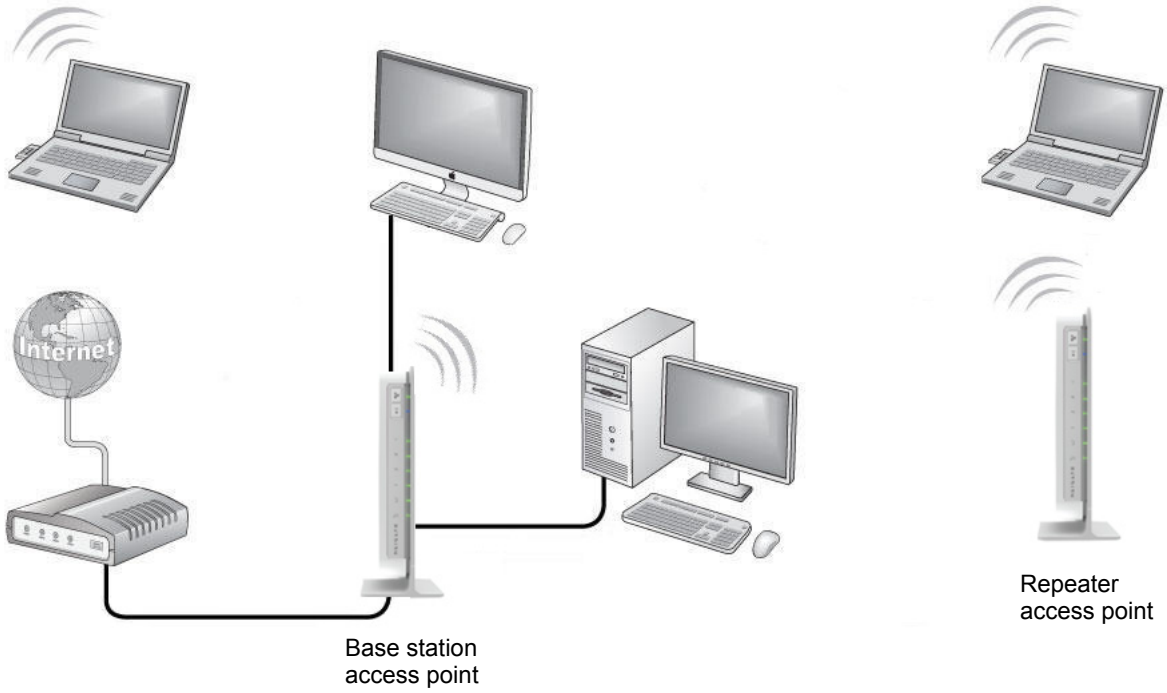


Figure 8. Wireless repeating scenario

Note: If you use the wireless repeating function, you need to select either **WEP** or **None** as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode **Up to 54 Mbps** in the Wireless Settings screen.

Wireless Base Station. The router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point.

Wireless Repeater. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

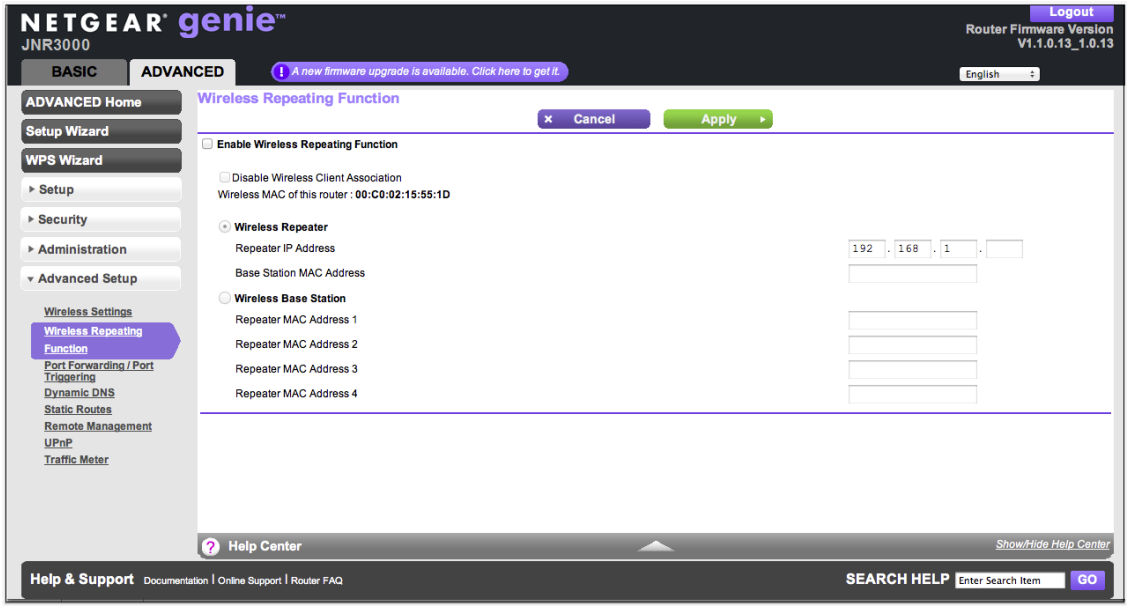
The JNR3000 router is always in dual band concurrent mode, unless you turn off one radio. Be aware that if you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless router or wireless base station, dual band concurrent mode is not affected.

For you to set up a wireless network with WDS, the following conditions have to be met for both access points:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) have to be configured to operate in the same LAN network address range as the access points.

Wireless Repeating Function

Select **Advanced > Advanced Setup > Wireless Repeating** to view or change wireless repeater settings for the router.



- **Enable Wireless Repeating Function**. Select the check box to use the wireless repeating function.
- **Wireless MAC of this router**. This field displays the MAC address for your router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your router is the repeater, select this check box.

Repeater IP Address. If your router is the repeater, enter the IP address of the other access point.

Disable Wireless Client Association. If your router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- If you are setting up a point-to-point bridge, select this check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

Base Station MAC Address. If your router is the repeater, enter the MAC address for the access point that is the base station.

- **Wireless Base Station**. If your router is the base station, select this check box.

  Disable Wireless Client Association. If your router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

  Repeater MAC Address (1 through 4). If your router is the base station, it can act as the "parent" of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

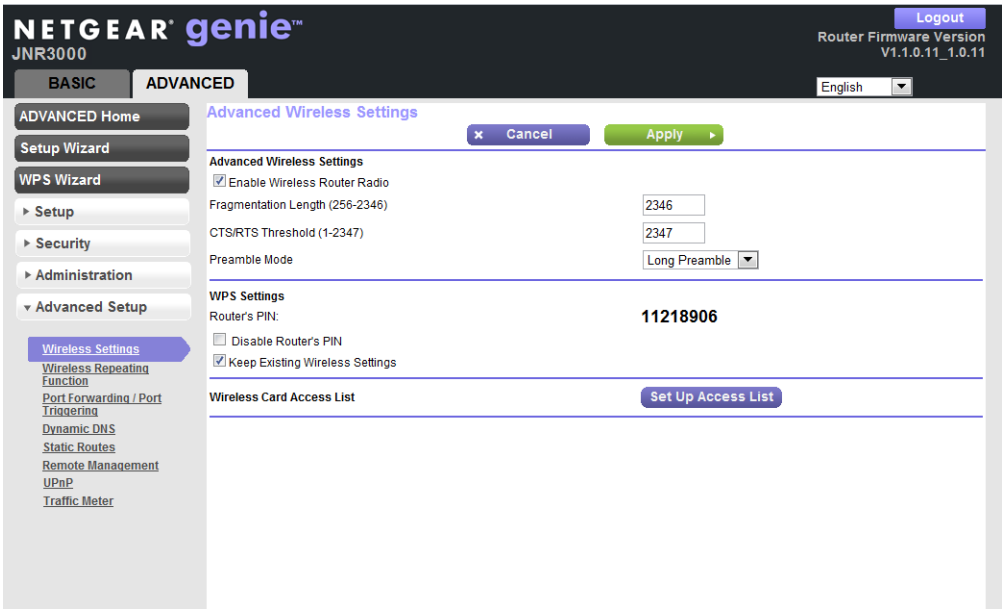
Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option has to be set to None or WEP.

2. Select **Advanced > Advanced Setup > Wireless Repeating Function** to display the Wireless Repeating Function screen.



3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

Note: If you are using the JNR3000 base station with a non-NETGEAR router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

➢ **To configure the router as a repeater unit:**

1. Log in to the router that will be the repeater. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
2. Select **Advanced > Wireless Repeating Function**, and select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.

3. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other access point.

Port Forwarding and Triggering

By default, the router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type **http://www.example.com** into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

   Source address. Your computer's IP address.

   Source port number. 5678, which is the browser session.

   Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

   Destination port number. 80, which is the standard port number for a web server process.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending

the web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

- The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
- The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the web server at www.example.com.

4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. The public IP address of your router.

   Destination port number. 33333.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. Your computer's IP address.

   Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the router, “When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address of www.example.com, which is the address of your router.

   Destination port number. 80, which is the standard port number for a web server process.

   The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does require that you know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

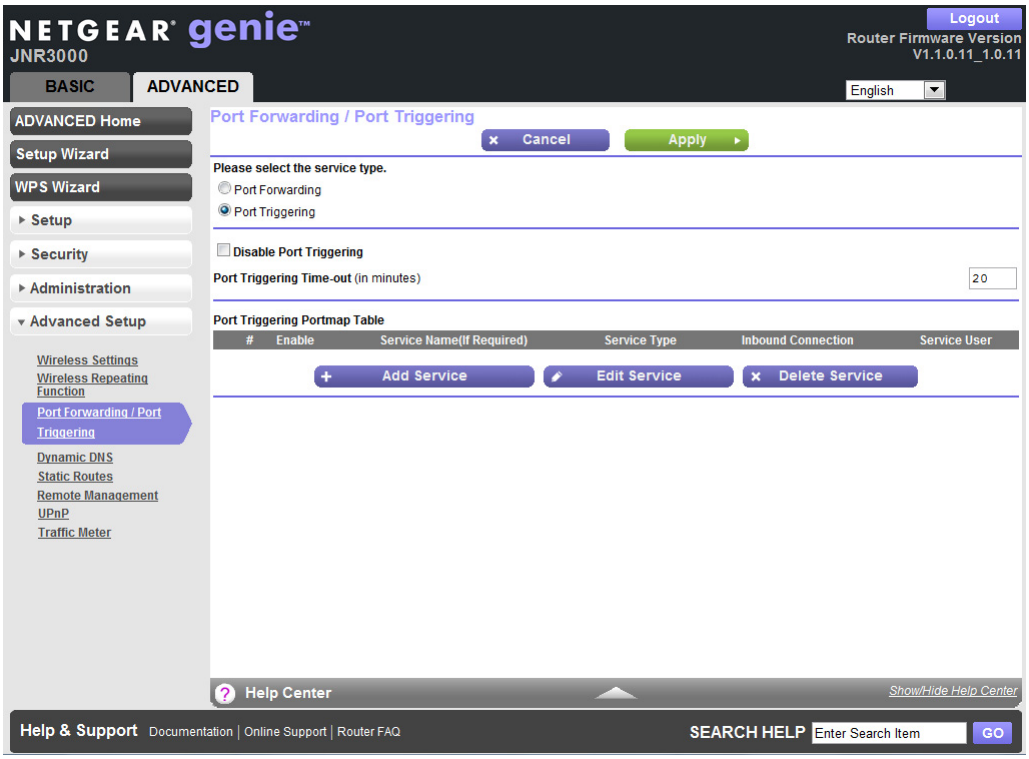
Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your JNR3000 router.

1. Select **Advanced Setup > Port Forwarding/Port Triggering** to display the following screen:



   Port Forwarding is selected as the service type.

2. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 73.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
4. Click **Add**. The service appears in the list in the screen.

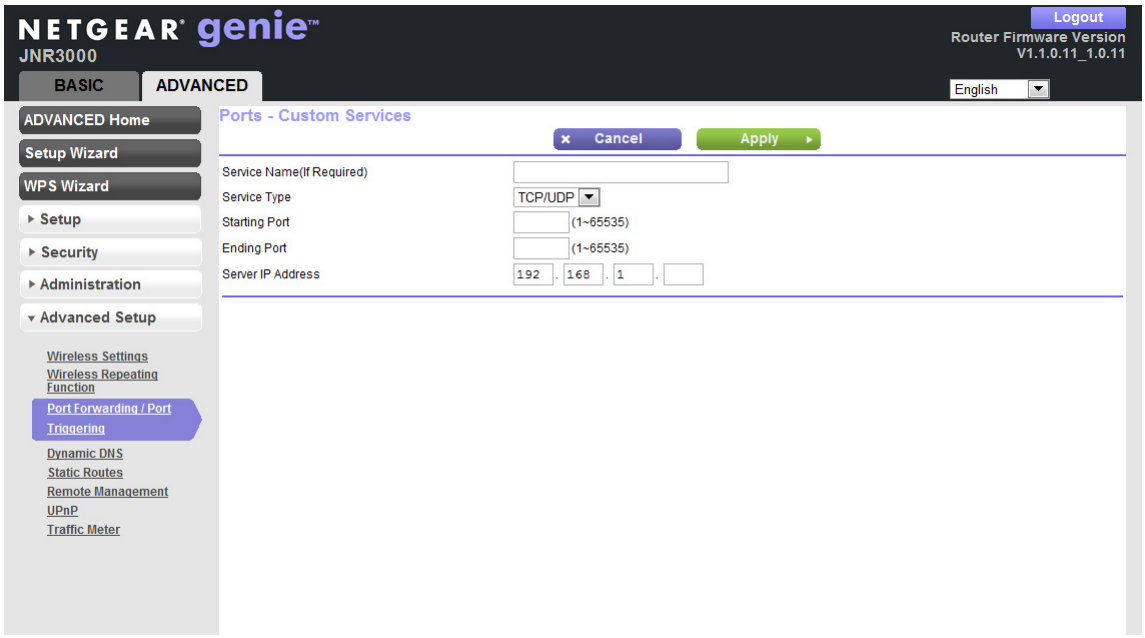
Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you have to first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To add a custom service:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.

3. Click the **Add Custom Service** button to display the following screen:



4. In the Service Name field, enter a descriptive name.
5. In the Protocol list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Starting Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the Ending Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
7. In the Server IP Address field, enter the IP address of your local computer that will provide this service.
8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Editing or Deleting a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your router will always give your web server an IP address of 192.168.1.33.
2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in *Dynamic DNS* on page 77. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound “trigger” port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

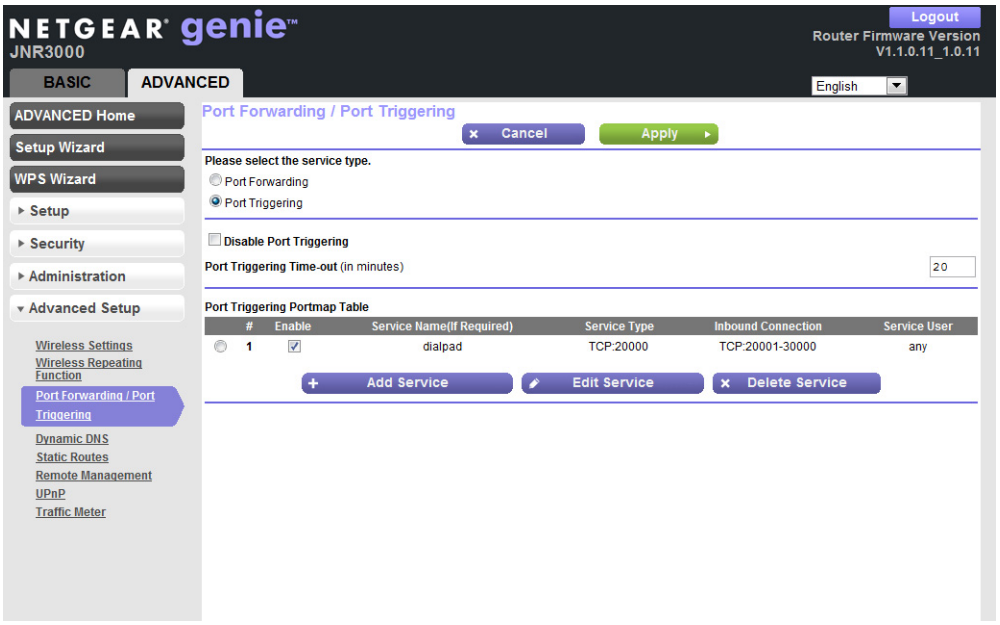
Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 82.

To set up port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To set up port triggering:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.

2. Select the **Port Triggering** radio button to display the port triggering information.

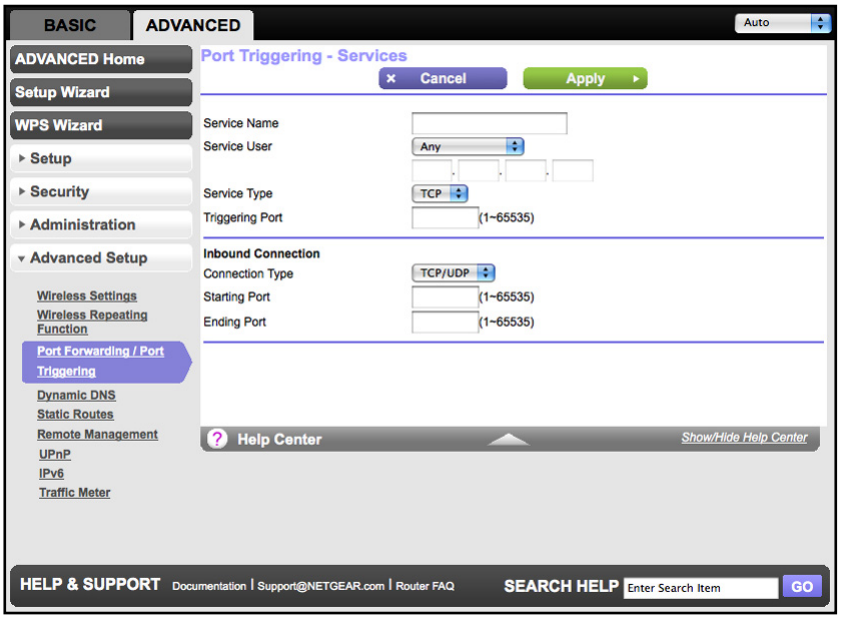


3. Clear the **Disable Port Triggering** check box if it is selected.

   Note: *If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.*

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes.
5. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

6. Click **Add Service** to display the following screen:



7. In the Service Name field, type a descriptive service name.
8. In the Service User list, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
9. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
10. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
11. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
12. Click **Apply**. The service appears in the Port Triggering Portmap table.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service will not work because private addresses are not routed on the Internet.

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and

host name that you configure in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at *http://hostname.dyndns.org*.

On the Advanced tab, select **Advanced Setup > Dynamic DNS** to display the following screen:

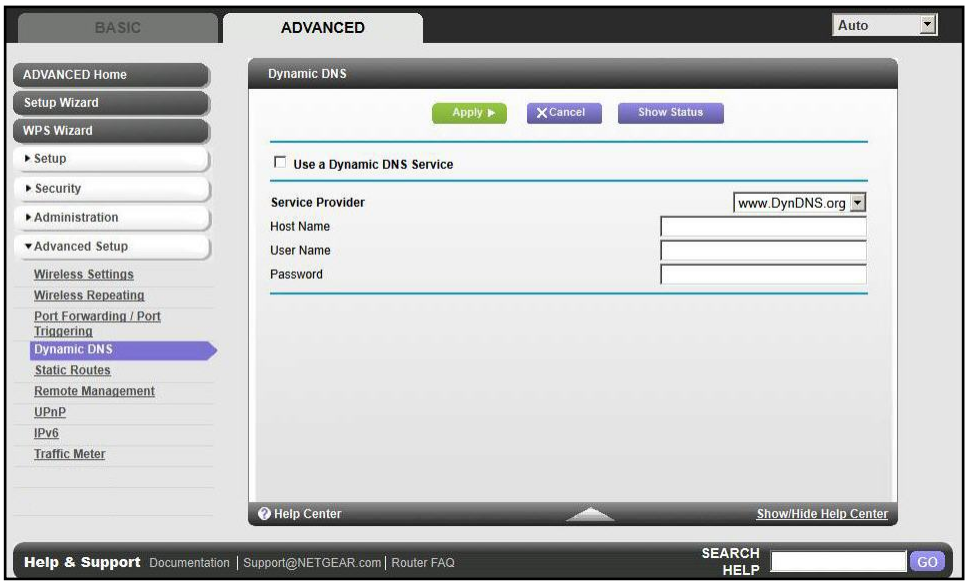


Figure 9. Forward traffic to a changing IP address

➢ **To set up Dynamic DNS:**

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list. For example, for DynDNS.org, select *www.dyndns.org*.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your Dynamic DNS service provider.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature.

   For example, the wildcard feature causes **.yourhost.dyndns.org* to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Static Routes

Static routes provide additional routing information to your router. Under usual circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

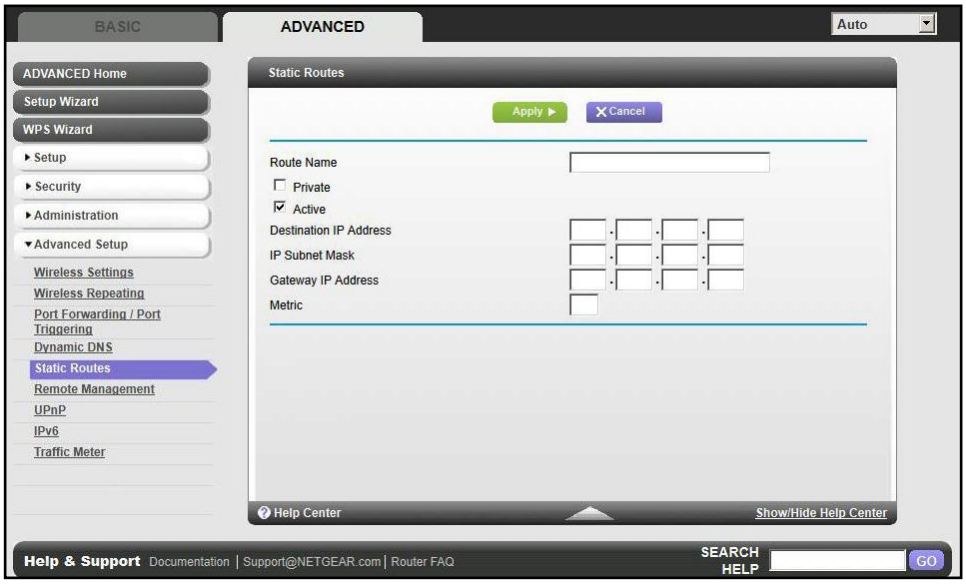
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **Advanced > Advanced Setup > Static Routes**, and click **Add** to display the following screen:



2. In the Route Name field, type a name for this static route (for identification purposes only.)
3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
4. Select the **Active** check box to make this route effective.
5. Type the destination IP address of the final destination.
6. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
7. Type the gateway IP address, which has to be a router on the same LAN segment as the JNR3000 router.
8. Type a number between 1 and 15 as the metric value.

   This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your JNR3000 router over the Internet.

➢ **To set up remote management:**

1. Select **Advanced > Advanced Setup > Remote Management**.

__Note:__ Be sure to change the router's default login password to a very secure password. The ideal password should contain no dictionary words from any language and contain uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the router's remote management.

__Note:__ For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number for accessing the management interface.

Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management nterface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.
6. When accessing your router from the Internet, type your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

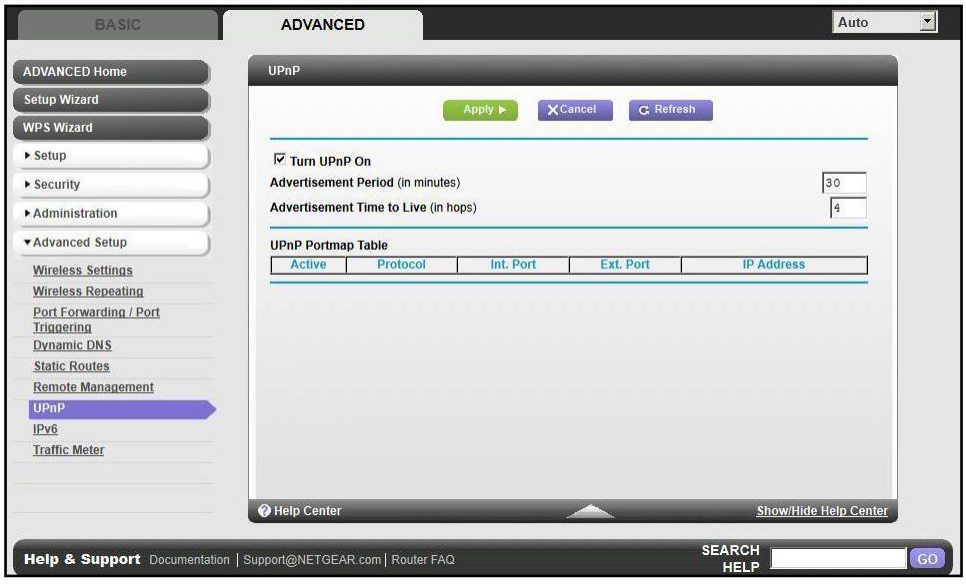
Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

1. Select **Advanced > Advanced Setup > UPnP**. The UPnP screen displays.



2. The available settings and information in this screen are:

   Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

   Advertisement Period. The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

   Advertisement Time to Live. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.

   UPnP Portmap Table. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

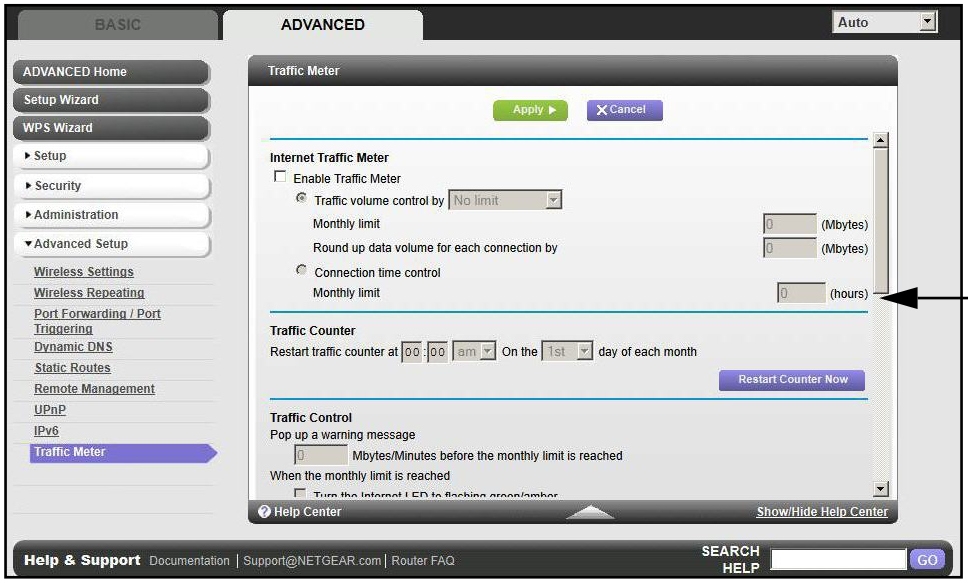
3. Click **Apply** to save your settings.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

To monitor Internet traffic:

1. Click **Advanced > Advanced Setup > Traffic Meter** to display the following screen:



2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:

   No Limit. No restriction is applied when the traffic limit is reached.

   Download only. The restriction is applied to incoming traffic only.

   Both Directions. The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.
5. Set the Traffic Counter to begin at a specific time and date.
6. Set up Traffic Control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.
7. Set up Internet Traffic Statistics to monitor the data traffic.
8. Click the **Traffic Status** button to get a live update on Internet traffic status on your router.
9. Click **Apply** to save your settings.

Troubleshooting

8

This chapter provides information to help you diagnose and solve any problems you mayencounter with your router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Restore the Factory Settings and Password*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router and computers.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the router and wait 2 minutes.
5. Turn on the computers.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

- The Internet LED on the router is on when the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.
- For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is on.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer must match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you must add the MAC address of each wireless computer to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers must have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshooting with the LEDs

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power/Test LED is on.
2. Verify that the Power/Test LED turns amber within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify that:
   - The Power/Test LED is solid green.
   - The Internet LED is on.
   - A numbered Ethernet port LED is lit for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

The LEDs on the front panel of the router can be used for troubleshooting.

Power/Test LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 12V DC, 1.5A power adapter that NETGEAR supplied for this product.
- If the Power/Test LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at *www.netgear.com/support.*

Power/Test LED Stays Amber

When the router is turned on, the Power/Test LED turns amber for about 20 seconds and then turns green. If the LED does not turn green, the router has a problem.

If the Power/Test LED is still amber 1 minute after you turn on power to the router:

1. Turn the power off and back on to see if the router recovers.
2. Press and hold the **Reset** button to return the router to its factory settings. as explained in *Restore the Factory Settings and Password* on page 93.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support.*

LEDs Never Turn Off

When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router.

If all LEDs are still on 1 minute after power-up:

- Cycle the power to see if the router recovers.
- Press and hold the **Reset** button to return the router to its factory settings as explained in *Restore the Factory Settings and Password* on page 93.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

Internet or Ethernet Port LEDs Are Off

If either the Ethernet port LEDs or the Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable:

  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Wireless LEDs Are Off

If the Wireless LEDs stay off, check to see if the Wireless On/Off button on the router has been pressed. This button turns the wireless radios in the router on and off. The Wireless LEDs are lit when the wireless radio is turned on.

The Push 'N' Connect (WPS) Button Blinks Amber

If after using the WPS function the button blinks amber, check the following:

- Make sure that you are using the button and not the router's built-in registrar.
- Check that PIN verification has succeeded for the wireless device you are adding to the wireless network.
- Make sure you have not pressed the WPS button on the side of the router after disabling the WPS feature (you logged in to the router and disabled this previously).
- Check that the router is not in the temporary AP setup locked state (if you are using the wireless repeater function).

Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. This procedure is explained in *Factory Default Settings* on page 96.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR router as an additional router behind an existing router in your network, consider replacing the existing router instead. NETGEAR does not support such a configuration.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services, for example, converting ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

➢ **To check the WAN IP address:**

1. Start your browser, and select an external site such as *www.netgear.com*.
2. Access the router interface at **www.routerlogin.net.**
3. Select **Adminstration > Router Status**.

4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in *Sequence to Restart Your Network* on page 86.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet Setup screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to clone your computer's MAC address.

If your router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address.You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address.

- You might be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Troubleshooting PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

➢ **To troubleshoot a PPPoE connection:**

1. Log in to the router.
2. Select **Administration > Router Status**.
3. Click **Connection Status**. If all of the steps indicate OK, then your PPPoE connection is up and working.

If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**. The router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshooting Internet Browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, check the following:

- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.

  Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer.

  Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- Your computer might not have the router configured as its default gateway.

  Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.

- You might be running log in software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

- Does the wireless device or computer that you are using find your wireless network?

  If not, check the Wireless LEDs on the front of the router. It should be lit. If it is not, you can press the **WiFi On/Off** button on the back of the router to turn the router's wireless radio back on.

  If you disabled the router's SSID broadcast, then your wireless network is hidden and does not show up in your wireless client's scanning list. (By default, SSID broadcast is enabled.)
- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **Wireless** see (*Basic Wireless Settings* on page 24).

  Note: *Be sure to click **Apply** if you make changes.*

Wireless Signal Strength

If your wireless device finds your network, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal blocked by objects between the router and your computer?

Restore the Factory Settings and Password

This section explains how to restore the factory settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see *Erase* on page 60).
- Use the Reset button on the back of the router. See *Factory Default Settings* on page 96. If you restore the factory settings and the router fails to restart, or the green Power/Test LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support at *http://www.netgear.com/support*.

Troubleshoot Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a network is made very easy by using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➢ **To ping the router from a running Windows PC:**

1. From the Windows toolbar, click **Start**, and then select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping www.routerlogin.net
3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections

  For a wired connection, make sure that the numbered LAN port LED is on for the port to which you are connected.

Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are on for the switch ports that are connected to your computer and router.

- Wrong network configuration

  Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

  Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button, and then select **Run**.
2. In the Windows Run window, type:

   ping -n 10 <*IP address*>

   where <IP address> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies like those shown in the previous section are displayed.

If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your router to "clone" or "spoof" the MAC address from the authorized computer.

Supplemental Information

This appendix provides factory default settings and technical specifications for the router.

- *Factory Default Settings*
- *Specifications*

Factory Default Settings

Table 3. Router Default Settings

Feature	Default Setting
Router Login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
Login name (case-sensitive)	admin (printed on product label)
Login password (case-sensitive)	password (printed on product label)
WAN MAC address	Default hardware address (on label)
MTU Size	1500
LAN IP address (gateway IP address)	192.168.1.1 (printed on product label)
Router subnet	255.255.255.0
DHCP server	Enabled
DHCP range	192.168.1.2 to 192.168.1.254
Time zone	GMT
Adjust for daylight saving time	Disabled
Allow a registrar to configure this router	Enabled
Wireless communication	Enabled
Preset SSID	NETGEAR*xx* (where *xx* is two random numbers). The Preset SSID is printed on the product label.
Security option passphrase	Enabled. The security option passphrase consists of an adjective, a noun, and three numbers. For example, luckyflower348. This passphrase is printed on the product label.
Wireless access list (MAC Filtering)	All wireless stations allowed
Broadcast SSID	Enabled
Transmission speed	Auto*
Country/Region	United States in NA only, otherwise varies by country and region
RF channel	auto until region selected
Operating mode	145 Mbps
Data rate	Best
Output power	Full
Inbound communication from the Internet	Disabled (bars unsolicited requests except traffic on port 80, the http port)
Outbound communication to the Internet	Enabled (all)

**. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.*

Specifications

Table 4. Router Technical Specifications

Feature	Specification
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, BigPond, Dynamic DNS, and UPnP
Power adapter	• North America: 120V, 60Hz, input • UK, Australia: 240V, 50Hz, input • Europe: 230V, 50Hz, input • China: 220V /60Hz, input • All regions (output): 12V DC @ 1.0A, output
Dimensions	6.8" x 4.6" x 1.4" 172.7 x 115.7 x 32.6 mm
Weight	0.48 lbs. 0.216 kg
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Designed to conform to the following standards	CCC SRRC FCC, CE
LAN	10BASE-T, 1000BASE-T, or 100BASE-Tx, RJ-45
WAN	10BASE-T , 1000BASE-T, or 100BASE-Tx, RJ-45

Notification of Compliance

B

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement, go to *ftp://downloads.netgear.com/files/GPLnotice.pdf*.

For GNU General Public License (GPL) related information, visit *http://support.netgear.com/app/answers/detail/a_id/2649*.

Interference Reduction Table

The following table shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	**Recommended Minimum Distance (in feet and meters)**
Microwave ovens	30 feet (9 meters)
Baby Monitor – Analog	20 feet (6 meters)
Baby Monitor – Digital	40 feet (12 meters)
Cordless phone – Analog	20 feet (6 meters)
Cordless phone – Digital	30 feet (9 meters)
Bluetooth devices	20 feet (6 meters)
ZigBee	20 feet (6 meters)

Index

A

access
  remote 81
  viewing logs 58
access points 64
accessing remote computer 68
adding
  custom service 73
  priority rules 42
address reservation 40
advertisement period 83
alerts, emailing 50
applications, QoS for online gaming 42
attached devices 23
authentication, required by mail server 51
automatic firmware checking 53
automatic Internet connection 32

B

back panel 13
backing up configuration 60
base station, setting up 66
blocking
  inbound traffic 68
  keywords 47
  services 48
  sites 47
box contents 10

C

cables, checking 86
changes not saved, router 92
compliance 98
configuration file 59, 60
configuring
  DMZ server 36
  Dynamic DNS 78
  NAT 35
  port forwarding 72
  port triggering 75
  QoS 41
  repeater unit 67
  user-defined services 48
connecting wirelessly 10
country setting 32
crossover cable 88
CTS/RTS Threshold 63
custom service (port forwarding) 73

D

dashboard 18
data packets, fragmented 36
default DMZ server 36
default factory settings, restoring 60, 93
default gateway 56
deleting
  configuration 60
  keywords 47
denial of service (DoS) protection 46
devices, attached 23
DHCP server 39, 56
DHCP setting 55
DMZ server 36
DNS addresses
  troubleshooting 90
DNS servers 68
Domain Name Server (DNS) addresses 22, 55
Dynamic DNS 77
DynDNS.org 77

E

email notices 50
encryption keys 28
erasing configuration 60
Ethernet cables, checking 86
Ethernet LED, troubleshooting and 87, 88

F

factory default settings, restoring 60, 93
factory settings
  resetting 13

firmware version 54
firmware, upgrading 17, 53
fragmentation length 63
fragmented data packets 36
front panel 11

G

games, online, QoS for 42
gateway IP address 22
Genie, NETGEAR 16
guest networks 27, 58

H

host name 21
host, trusted 47

I

inbound traffic, allowing or blocking 68
installing NETGEAR Genie 16
installing with the Setup Wizard 32
Internet connection
    setting up 21
    troubleshooting 89
Internet LED, troubleshooting and 87
Internet port 32, 54
Internet Relay Chat (IRC) 70
Internet service provider (ISP)
    account information 15
    Internet Setup screen 21
    login 15
Internet services, blocking access 48
Internet Setup screen 21
interval, poll 55
IP addresses
    current 54
    DHCP 15
    dynamic 77
    reserved 40
IP subnet mask 55

K

keywords 47

L

label, product 13
LAN port
    QoS for 43
    settings 54
LAN setup 38
language setting 32
lease, DHCP 56
LEDs
    described 12
    troubleshooting and 87
local servers, port forwarding to 72
logging in 15, 17
logs
    emailing 50
    viewing 58

M

MAC addresses
    current 54
    product label 13
    QoS for 44
mail server, outgoing 51
maintenance settings 52
managing router remotely 81
menus, described 18
metric value 80
mixed mode security options 28
MTU size 36
multicasting 39

N

NAT (Network Address Translation) 35, 36, 69
NETGEAR Genie 16
network, how to restart 86
networks
    guest 58
networks, guest 27
networks, troubleshooting 86

O

outgoing mail server 51

P

packets, fragmented 36
Parental Controls 24
passphrases
  changing 26
  product label 13
password recovery, admin 61
password, restoring 93
poll interval 55
port filtering 48
port forwarding 68, 71, 72
port numbers 48
port status 55
port triggering 68, 69, 72, 75
ports,listed, back panel 13
positioning the router 10
Power LED, troubleshooting and 87
PPPoE (PPP over Ethernet) 90
Preamble mode 63
preset security
  about 24
  passphrase 26
pre-shared key 28
primary DNS addresses 22
prioritizing traffic 41
Push 'N' Connect 19

Q

QoS (Quality of Service) 41

R

radio, wireless 63
range of wireless connections 10
recovering admin password 61
releasing connection status 56
remote management 81
renewing connection status 56
repeater units 67
reserved IP adresses 40
restarting network 86
restoring
  configuration file 60
  default factory settings 60, 93
router interface, described 18
router status, viewing 54

S

scheduling keyword and service blocking 50
secondary DNS 22
security 24
  firewall settings 46
  see also security options
security options 28
security PIN 13, 33
sending logs by email 50
serial number, product label 13
services, blocking 48
settings, default. *See* default factory settings
Setup Wizard 32
sites, blocking 47
SMTP server 51
specifications
  technical 95
SSID, described 26
static routes 79
status, router, viewing 54
subnet mask 55
system up time 55

T

technical specifications 95
technical support 2
Temporal Key Integrity Protocol (TKIP) 28
time to live, advertisement 83
time-out, port triggering 76
trademarks 2
traffic metering 83
troubleshooting 85
  log in access 89
  router changes not saved 92
trusted host 47

U

Universal Plug and Play (UPnP) 82
up time, system 55
upgrading firmware 17, 53
user-defined services 48

V

viewing
  logs 58
  router status 54

W

WAN IP address, troubleshooting 89
WAN setup 35
Wi-Fi Protected Setup (WPS) 19, 33
    devices, adding 19
wireless channel 26
wireless connection, troubleshooting 92
wireless connections 10
wireless devices,adding to the network 19
Wireless Distribution System (WDS) 64, 65
Wireless LED, troubleshooting and 88, 89
wireless mode 26
wireless network name (SSID)
    broadcast 25
    described 26
    product label 13
wireless network settings 26
wireless radio 63
wireless repeating 64, 65
    base station 66
    repeater unit 67
wireless security options 28
wireless settings 24, 58
    checking for correct 86
    NETGEAR badge LED 26
    SSID broadcast 25
WMM (Wi-Fi Multimedia) 41
WPA encryption 28
WPA2 encryption 28
WPA2-PSK encryption 28
WPA-PSK/WPA2-PSK mixed mode 28
WPS button 19
WPS-PSK encryption 28
WPS-PSK+ WPA2-PSK encryption 28